CERIAS Tech Report 2007-90

grating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Pra

by J. Ekstrom, Melissa Dark, and Barry Lunt
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice

Melissa Jane Dark
Purdue University, West Lafayette, Indiana

Joseph J. Ekstrom, Barry M. Lunt
Brigham Young University, Provo, Utah

dark@purdue.edu jekstrom@byu.edu luntb@byu.edu

Executive Summary

In December 2001 a meeting of interested parties from fifteen four-year IT programs from the US along with representatives from IEEE, ACM, and ABET (CITC-1) began work on the formalization of Information Technology as an accredited academic discipline. The effort has evolved into SIGITE, the ACM SIG for Information Technology Education. During this period three main efforts have proceeded in parallel: 1) Definition of accreditation standards for IT programs, 2) Creation of a model curriculum for four-year IT programs, and 3) Description of the characteristics that distinguish IT programs from the sister disciplines in computing.

During the deliberations of the SIGITE Curriculum Committee, several topics emerged that were considered essential, but that did not seem to belong in a single specific knowledge area or unit. One of the most significant of these "pervasive themes" is Information Assurance and Security (IAS). A consensus emerged that these themes must be addressed during the entire learning experience and that students and instructors need to be constantly aware of how these themes are woven through the fabric of the curriculum.

In this paper we present an introduction to SIGITE and the context of the work of the Curriculum Committee on IT2005, the IT curriculum volume described in the Overview Draft document of the Joint Task Force for Computing Curriculum 2005. We then describe the IAS component of the IT2005 document and how some IT programs are incorporating IAS as a "pervasive theme" that is woven through the curriculum. We conclude with some observations about the experience and some suggestions for those attempting to integrate information assurance and security into an existing program.

Keywords: Information Assurance, Information Technology, CC2005, IT2005, Education, IT, IA, IAS, Pervasive Themes

Introduction

In December 2001 a meeting (CITC-1) of interested parties from fifteen four-year IT programs from the US along with representatives from IEEE, ACM, and ABET began work on the formalization of Information Technology as an accredited academic discipline. The effort has evolved into SIGITE, the ACM SIG for Information Technology Education. During this evolution three main efforts have proceeded in parallel: 1) Definition of accreditation standards for IT programs, 2) Creation of a model curriculum for four-year IT programs, and 3) Description of the characteristics that distinguish IT programs from the sister disciplines in computing.

One of the biggest challenges during the creation of the model curriculum was understanding and presenting the knowledge area that was originally called "security". Some of us were uncomfortable with the term because it was not broad enough to cover the range of concepts that we felt needed to be covered. We became aware of a community that had resolved many of the issues associated with the broader context we were seeking, Information Assurance. Information assurance has been defined as "a set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (National Security Agency, http://www.nsa.gov/ia/iaFAQ.cfm?MenuID=10#1). The IA community and work done by IA educators became useful in defining requisite security knowledge for information technology education programs.

We believe that the Information Technology Education and the Information Assurance Education communities have much to share with each other and with other computing disciplines. Over the last several months we have been presenting our evolving work at various conferences. At the 9th Colloquium for Information System Security Education in Atlanta we introduced CC2005 and IT2005 to the IA Education community (Ekstrom & Lunt, 2005). At SIGITE 2005 we presented additional results (Dark, Ekstrom & Lunt, 2005). We have also introduced these concepts to the EET community at ASEE 2006 and reported additional results at the 10th Colloquium for ISSE in Adlephi (Dark, Ekstrom & Lunt, 2006a, 2006b). In the current paper we introduce the history and current state of IT2005 and IA education to the larger IT education community. We describe how significant concepts from the Information Assurance community have been integrated into IT2005 as a "pervasive theme". We then describe how some IT programs are integrating IAS concepts into existing programs and conclude with some observations about how computing programs might begin introducing important information and security into an existing curriculum.

CC2005 and IT2005

In the first week of December of 2001 representatives from 15 undergraduate information technology (IT) programs from across the country gathered together near Provo, Utah, to develop a community and begin to establish academic standards for this rapidly growing discipline. This first Conference on Information Technology Curriculum (CITC-1) was also attended by representatives from two professional societies, the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers, Inc. (IEEE), and also the Accreditation Board for Engineering and Technology, Inc. (ABET). This invitational conference was the culmination of an effort begun several months earlier by five of these universities who had formed a steering committee to organize a response from existing IT programs to several initiatives to define the academic discipline of IT. The steering committee wanted to ensure that the input of existing programs played a significant role in the definition of the field.

A formal society and three main committees were formed by the attendees of CITC-1. The society was the Society for Information Technology Education (SITE); one of the committees formed was the executive board for SITE, composed of a president, vice-president, secretary, treasurer, regional representatives, and an activities chairperson. The other two committees formed were the IT Curriculum Committee, including subcommittees for 4-year and 2-year programs, and the IT Accreditation Committee, also including subcommittees for 4-year and 2-year programs.

It should be acknowledged here that IT has two substantially different interpretations, and that these should be clarified. Information Technology (IT) in its broadest sense encompasses all aspects of computing technology. IT, as an academic discipline, focuses on meeting the needs of users within an organizational and societal context through the selection, creation, application, integration and administration of computing technologies. A more detailed history of SIGITE is available elsewhere in this special issue of JITE.

SIGITE is directly involved with the Joint Task Force for Computing Curriculum 2004 and has 2 representatives on the task force. This task force is a continuation of the effort that created CC2001 (Joint Curriculum Committee, 2001) the current computer science curriculum standard. CC2001 has been relabeled CS2001 and the current draft of the CC2005 Overview document (Joint Curriculum Committee, 2005) presents the structure being used to describe computing and its sub-disciplines (See Figure 1). The SIGITE Curriculum Committee is responsible for IT2005, the Information Technology Curriculum Volume. IT2005 was made available for comment in mid 2005 (SIGITE Curriculum Committee, 2005)

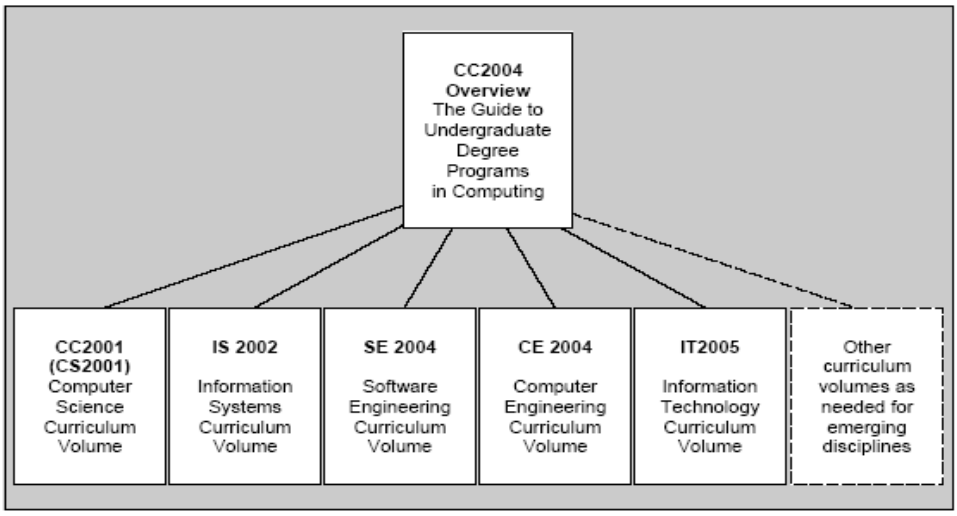

Figure 1: Computing Curricula Structure

Information Assurance Education

Information assurance education includes all efforts to prepare a workforce with the needed knowledge, skills, and abilities to assure our information systems, especially critical national security systems. Information assurance education has been growing in importance and activity for the past two decades. A brief look at the involved entities and history will shed light on the growth.

The National Information Assurance Education and Training Partnership (NIETP) program, created in 1990, is a partnership among government, academia and industry focused on advancing information assurance education, training, and awareness. The NIETP serves in the capacity of national manager for information assurance education and training related to national security systems and coordinates this effort with the Committee on National Security Systems (CNSS). "The CNSS provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems. National security systems are information systems operated by the U.S. Government, its contractors or agents that contain classified information or that:

- involve intelligence activities;
- involve cryptographic activities related to national security;
- involve command and control of military forces;
- involve equipment that is an integral part of a weapon or weapons system(s); or
- are critical to the direct fulfillment of military or intelligence missions (not including routine administrative and business applications)." http://www.cnss.gov/history.html (NSA, 2006a)

Education and training standards are among the many standards and guidelines that CNSS issues. The training/education standards issued to date include: a) NSTISSI 4011 – The National Training Standard for Information Systems Security Professionals, b) CNSSI 4012 – The National Information Assurance Training Standard for Senior Systems Managers, c) CNSSI 4013 – The National Information Assurance Training Standard for System Administrators, d) CNSSI 4014 - Information Assurance Training Standard for Information Systems Security Officers, and e) CNSSI 4015 – The National Training Standard for Systems Certifiers. CNSSI 4016 – The National Training Standard for Information Security Risk Analysts.

The NSTISSI-CNSSI standards referenced above have been used to develop in-service training and education opportunities for enlisted and civilian employees in an effort to assure quality preparation of professionals entrusted with securing our critical information. In addition, the NSTISSI-CNSSI standards have also been deployed to colleges and universities in an effort to also prepare qualified individuals pre-service. The most significant effort to involve colleges and universities has been through the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program. The CAEIAE program was started in 1998 by the National Security Agency (NSA) and is now jointly sponsored by the NSA and the Department of Homeland Security. The purpose of the program is to recognize colleges and universities for their efforts in information assurance education and also to encourage more colleges and universities to develop courses and programs of study in information assurance. In order to be eligible to apply for CAEIAE certification, an institution must first demonstrate that it meets the 4011standard and a minimum of one other standard. Once an institution is eligible to apply, then it must meet the following criteria to earn the CAEIAE designation: a) evidence of partnerships in IA education, b) IA must be treated as a multidisciplinary science, c) evidence that the university encourages the practice of information assurance in its operations, d) demonstration of information assurance research, e) demonstration that the IA curriculum reaches beyond physical geographic borders, f) evidence of faculty productivity in information assurance research and scholarship, g) demonstration of state of the art information assurance resources, h) a declared concentration(s) in information assurance, i) a university recognized center in information assurance, and j) dedicated information assurance faculty (http://www.nsa.gov/ia/academia/caeCriteria.cfm?MenuID=10.1.1.2) (NSA, 2006b)

In 1999, there were seven institutions designated as the inaugural CAEIAE schools. The certification is good for three years at which time institutions can reapply. An additional 6-10 institutions are awarded the certification every year; today, there are more than 70 CAEIAE institutions. The types of institutions and programs that are applying and being certified are growing not just in number, but also in diversity. In the first round of certification, the institutions were largely research institutions and their respective programs were at the graduate level in computer science. Today, institutions are certifying courses at the undergraduate level in computer science, management information systems, and information technology. The work being done by SIGITE is important to the further expansion of information assurance education as information assurance expands beyond the development of information systems to include the entire system life cycle including deployment, operation, maintenance, and retirement of such systems.

As a Center for Academic Excellence in Information Assurance Education, Purdue University, and more specifically the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University, has taken an active role in building partnerships in IA education. In 2002 faculty at CERIAS were awarded a grant from the National Security Agency to develop a national faculty development program to increase faculty capacity to teach information assurance and security in multiple disciplines. The program that resulted was an 8 week, 11 credit hour information assurance education graduate certificate (IAEGC) program for faculty from across the nation. The goals of faculty development program are to: 1) develop faculty expertise in information assurance and security, and 2) develop pedagogical knowledge and skills that faculty need to implement IA courses and modules into their academic programs. The results of faculty development include: capacity

building, curriculum development and implementation, academic papers, grant proposals, etc. To date, IAEGC has resulted in 76 new courses developed by faculty who attended IAEGC. Furthermore, 46 existing courses were modified to include more information assurance and security. To date, 4,893 students have enrolled in these courses.

However, there was also another outcome that is perhaps more significant than the innovations at the course level; that was the development of information assurance and security as a knowledge area in information technology education. This outcome was a result of the participation of one of the curriculum co-authors in the IAEGC program. It is significant because including IAS as a knowledge area in the IT body of knowledge has the ability to influence curricula across institutional and national boundaries, and also for a longer period of time. In addition, the addition of IAS into the IT curriculum represents the first significant effort to address IAS as a defined subfield within a discipline. It is also the first formal effort by post secondary educators to derive a core body of knowledge in IAS with the intent of using it during accreditation; in contrast, the NSA efforts to define IAS knowledge and skill requirements are largely driven by government needs and are NOT accreditation guidelines.

Information Assurance in IT2005

The IT2005 volume is modeled on CS2001. It consists of 12 chapters and 2 appendices. The current draft resides at http://sigite.acm.org/activities/curriculum/ (SIGITE Curriculum Committee, 2005)

Chapters 5 and 7 are of particular interest for this discussion. Chapter 5 is an overview of the IT body of knowledge. A summary is included as Appendix A. Chapter 7 discusses the relationship of the core topics described in the body of knowledge to IT curriculum. IAS is explicitly mentioned in three contexts:

- Section 7.2 as part of the IT Fundamentals Knowledge Area (KA)
- Section 7.2 as a "pervasive theme"
- Section 7.4 as a KA that integrates the IAS concepts for students ready to graduate.

A knowledge area represents a significant body of knowledge in a discipline. Knowledge areas are enacted as courses and curriculum and allow curricular and course differences from institution to institution while still addressing the need for a common body of knowledge to be addressed at the programmatic level. Pervasive themes are topics that should permeate the IT curriculum, i.e., they cut across all knowledge areas.

Information Assurance and Security is the only area that is an IT Fundamental, a "pervasive theme" and also a complete knowledge area with a recommended senior level course for integrating all of the concepts. Clearly, IT2005 presents Information Assurance and Security as a core competency required by every graduate of an IT program.

During the early analysis of IT as an academic discipline, Delphi studies were performed that ranked "Security" as a central area for IT. (Ekstrom, et. al., 2006) As we studied the issues several members of the committees involved were uncomfortable with "security" as the name for the knowledge area. The name seemed too restrictive. We discovered that NSA had begun to use the umbrella term Information Assurance (NSA, 2006d) to cover what we were calling security. Even though this term is defined to cover exactly what the IT community meant by security, the use of the terminology elicited a lot of blank stares. We found that explicitly adding security to the name of the knowledge area eliminated much of the confusion. We are indebted to the Center for Education and Research for Information Assurance and Security (CERIAS, 2006) at Purdue whose name provided the inspiration to use IAS as a name for the knowledge area.

Once the naming issue was resolved, the SIGITE curriculum committee struggled to find a model for IAS that could form the basis for a "pervasive theme". The model needed to:

- be understood by freshman IT students
- provide a framework to integrate IAS concepts that are integrated into nearly all of the other KAs
- be rich enough to support a senior level course that ties everything together.

When *A Model for Information Assurance: An Integrative Approach* (Machonachy, et al., 2001) was introduced to the writing committee, consensus on a model was achieved. The model is a cube (see Figure 2) that provides a simple visual representation that a freshman can understand, yet the 3 dimensional structure facilitates the detailed analysis required for use in technology specific contexts, and is comprehensive enough to encompass a capstone learning experience.

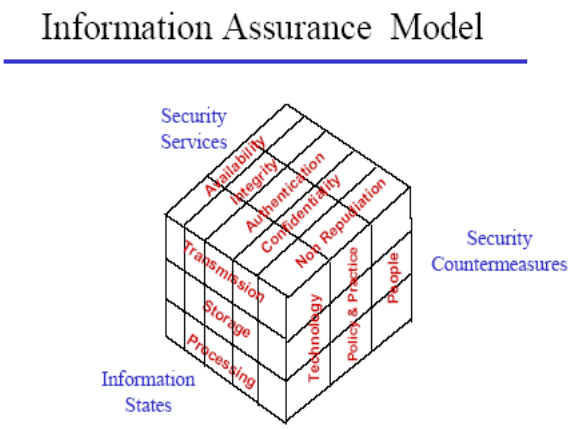

Figure 2: The IA Cube (Machonachy, et al., 2001)

Security is often discussed in terms of individual hacks, coding practices, vulnerabilities in protocol design, strong and weak passwords, or cryptographic algorithms. This practice provides no context within which to understand the relationships between the concepts. Students are left to swim around in a sea of seemingly disconnected concepts. The "cube" provides a basic vocabulary, along with a set of relationships between the concepts represented by the vocabulary, that allows the instructor to build a basic learning structure for students in a one hour lecture. IT2005 uses this model with its associated vocabulary and relationships to structure IAS concepts throughout the document.

"Pervasive Themes" in IT2005

During the deliberations of the SIGITE Curriculum Committee, several topics emerged that were considered essential, but that did not seem to belong in a single specific knowledge area or unit. These topics, referred to as pervasive themes, are:

- user advocacy
- information assurance and security
- ethics and professional responsibility
- the ability to manage complexity through: abstraction & modeling, best practices, patterns, standards, and the use of appropriate tools
- a deep understanding of information and communication technologies and their associated tools
- adaptability

- life-long learning and professional development
- interpersonal skills

The committee states "that these topics are best addressed multiple times in multiple classes, beginning in the IT fundamentals class and woven like threads throughout the tapestry of the IT curriculum" (SIGITE Curriculum Committee, 2005).

These themes need to be made explicit in the minds of the students and the faculty. The themes touch many of the topics throughout the curriculum. Every time a new technology is announced in the media, an instructor has the opportunity to drive home the importance of "life-long learning". Every time there is a cyber-crime in the media we have the opportunity to discuss the ethical and professional ramifications. It is recommended that an IT Fundamentals course be taught early in the curriculum where all of these themes are introduced and discussed as concepts that touch everything an IT professional does.

Each of these topics deserves a full treatment; however, for the purposes of this paper we will focus on IAS, possibly the most pervasive theme. We will address approaches to achieve addressing IAS "multiple times in multiple classes" below.

The Information Assurance and Security Knowledge Area

In early 2003, the SIGITE curriculum committee divided into working groups around the knowledge areas to make an initial cut at the list of topics for each KA. A significant revision was accomplished and reviewed by the participants at the 2004 IAEGC program at Purdue in August 2004. The list of areas for the IAS KA was finalized in late 2004 at a full IT Curriculum Committee meeting. The draft of the completed IAS KA was completed in early Feb 2005 by the IAS working group, edited by the writing committee in late Feb 2005 and was presented to the full committee in April 2005.

Figure 3 is a list of the IAS KA and its topics. The numbers in parenthesis are the number of lecture hours the committee thought would be required to give an IT student minimum exposure to the unit. The basic structure and vocabulary is derived directly from work done in the IA community (Machonachy, et. al., 2001). It should be noted that the ordering of units in all of the KAs, is first "Fundamentals", if there is one, and then the units are sorted in order of the number of core hours. This ordering should not be considered as any indication of the order the units would be covered pedagogically in an implemented curriculum.

IAS. Information Assurance and Security (23 core hours)
- **IAS1. Fundamental Aspects (3)**
- **IAS2. Security Mechanisms (countermeasures) (5)**
- **IAS3. Operational Issues (3)**
- **IAS4. Policy (3)**
- **IAS5. Attacks (2)**
- **IAS6. Security Domains (2)**
- **IAS7. Forensics (1)**
- **IAS8. Information States (1)**
- **IAS9. Security Services (1)**
- **IAS10. Threat Analysis Model (1)**
- **IAS11. Vulnerabilities (1)**

Figure 3: IAS Knowledge Area Topics

A summary of the IAS KA is in Appendix A, and a complete treatment is found in IT2005 (SIGITE Curriculum Committee, 2005) including topics, core learning outcomes, and example elective learning outcomes.

In reviewing this model curriculum for IAS in Information Technology, it should be remembered that the core topics and associated lecture hours are the minimum coverage that every IT student in every program should receive. We would expect that most institutions would provide additional instruction in Information Assurance and Security according to the strengths/areas of specialization in their programs of study.

Integrating IAS into the Existing Brigham Young University Curriculum

The Brigham Young University curriculum has evolved into what IT2005 calls a "core/integration first" approach. As described in IT2005, an IT curriculum may be implemented using one of several implementation strategies. The strategies are practicum first, theory first, core/integration first and pillars first (IT2005, Section 6.3) During this evolution, significant portions of the introductory material in operating systems, databases, web systems, networking had been moved to lower division courses by early 2004. Much of the shift occurred when the introduction to web systems was moved from the junior to the sophomore year and introductory material sufficient to understand web systems was included for networking, databases, operating system administration and OS process models. The improvements in flow and reduced redundancy have been noticeable in the upper division core courses. Appendix B graphs the current Brigham Young University course structure. In late 2004 and early 2005 we began implementing the "pervasive theme" of IAS in earnest.

A senior level IAS class had been introduced into the curriculum in early 2004 and was made a requirement in 2005. However, we recognized that simply adding a required course at the end of a student's college experience would not be adequate. SIGITE discussions had placed security in the pervasive theme category at the very beginning, though the name of the KA wasn't chosen until 2004. We were faced with the challenge of integrating the IAS fundamentals into the introductory courses, morphing the security modules in the existing classes to use the MSRW framework (Machonachy, et al., 2001) and bringing all of the students in the program up to speed on the new framework simultaneously.

Our approach has been to prepare one hour modules on the MSRW framework that can be used in an existing course to bring students up to speed or taught in seminars as needed. We are in the process of integrating the IAS Fundamentals into our introductory courses. We successfully integrated the IAS modules into the sophomore introduction to web-based systems course, which was already introducing all of the major IT areas. The course was modified to replace a 3 week team project experience with a 2 week team oriented lab and then using the time for IAS topics. Much remains to be done, but the initial experience is positive. The faculty seems unified in their desire to implement IAS as a pervasive theme. For example, 2 lecture and 2 lab hours are now included in the computer communications course, and 3 lecture hours and 3 lab hours were added to the web systems course. The IAS component of the database course was rearranged and strengthened with 1 lecture hour added. Similar adjustments have been made throughout the curriculum.

Integrating IAS into the Existing Purdue University Curriculum

Two senior level IAS classes have been introduced into the curriculum at Purdue University. The first is entitled Network Security and the second is Introduction to Cyberforensics. There is also a Biometrics course offered in another department that CIT students at Purdue University can take. In addition, Purdue is currently developing an Applied Cryptography class for undergraduates. The combination of

these four courses addresses most of the topics outlined in the Information Assurance and Security knowledge area of IT 2005. However, some of the fundamental aspects (IAS1) and operational issues (IAS3) are covered as topics in introductory and intermediate courses, which helps fulfill the prescription that IAS also be a pervasive theme.

In addition, the IAS courses serve the purpose of helping students achieve program outcomes. At Purdue University we have found that our IAS courses map to the following IT program outcomes.

General student outcomes:

- ability to apply knowledge of computing and mathematics appropriate to the discipline;
- ability to function effectively on teams to accomplish a common goal;
- Understanding of professional, ethical and social responsibilities;
- ability to analyze the impact of computing on individuals, organizations and society, including ethical, legal, security and global policy issues;
- recognition of the need for, and an ability to engage in continuing professional development;
- ability to use current techniques, skills, and tools necessary for computing practice.
- Specific student outcomes:
- ability to use and apply current technical concepts and practices in core information technologies;
- understanding of best practices and standards and their application;
- ability to assist in the creation of an effective project.

IAS at other Institutions

The most common way to add a topic to a curriculum is to add a course on that topic. Therefore, it comes as no surprise that most institutions which are including IAS in their IT curriculum have done so by adding an elective in this area. Some of these courses focus on network security, some on computer system security, and some on forensics, but all are available to all undergraduate students. While this is highly commendable, and surely is one essential step to fully making IAS part of the IT curriculum, there is more to be done to comply with the accreditation standards.

Care should be taken to cover all of the required topics in courses that are required of all IT students, elective coverage of IAS is not enough. Each required IT course must be considered with an eye to where IAS should be covered. Where such opportunities are found, the program must define and create small modules that can be used in the above opportunities, and to make sure they become part of the curriculum. We acknowledge that the seamless integration of IAS throughout an existing curriculum is no small feat. It requires considerable coordination of faculty and courses. However, given the nature of IAS, this approach would provide the most meaningful learning experience for students.

Interdisciplinary courses and programs are also worth considering when implementing IAS into the curriculum. IAS is, by nature, an interdisciplinary field. It incorporates aspects of computer science, engineering, information technology, psychology, criminology, law, management, and sociology. Relevant courses in other disciplines as well as co-taught courses would be an effective way to integrate IAS into the IT curriculum.

It is our opinion that IAS must be integrated into the entire IT curriculum. Why? IAS is a growing problem and, to a large extent, it is a social issue. One of the most effective ways to address social problems is through social milieus (social structures, communities, education, etc.) and with social solutions (e.g., policies, laws, codes of conduct, knowledge, etc.) The choice to NOT integrate IAS into the curriculum is, in our opinion, negligent. Pragmatically speaking, the growth of this social problem can be seen in the increase of IAS jobs.

We also believe that IAS in an excellent way to enable problem-based learning in the curriculum. Problem-based learning, when done effectively, can have several positive effects. Problem-based learning can increase students' ability to think critically, transfer knowledge to new situation, and solve ill-define problems. Furthermore, problem-based learning can increase students' motivation to learn.

Conclusion

Information Technology is maturing rapidly as an academic discipline. A public draft of the IT volume described in the Computing Curriculum 2005 Overview is ready for review. The SIGITE Curriculum Committee is soliciting feedback on the document. This paper presents a brief history of SIGITE, the ACM SIG for Information Technology Education, and a brief introduction to the Information Assurance Education community. We have discussed the integration of Information Assurance and Security concepts into IT2005 as a "persistent theme" and have given examples of how existing IT programs have integrated IAS concepts into their curriculum.

In conclusion, we believe that a weakness in many computing programs is the treatment of security topics throughout the curriculum. The IT2005 model curriculum has benefited significantly through collaboration with members of the Information Assurance Education community. It is an axiom of system development that security is built in more effectively that it is added on. The IT2005 curriculum document requires that IAS be treated throughout the curriculum and we have given examples of how this can be accomplished. To summarize the approaches we have discussed we present the following as general approaches to the problem.

1. Slip-streaming: This approach requires the opportunistic insertion of current events into discussions in the existing curriculum. For example, during a discussion of C I/O one could take 5 minutes and discuss how one of the SMTP buffer-overflow problems allowed a root kit to insert its code into a buffer and execute it because the code assumed that no one would ever enter more than 2000 characters without an end of line. It would also be wise to point out that one should probably never use unbounded routines like "gets" and "puts" in production code because you are creating potential buffer overflow conditions every time they are used.
2. Mini-topics: This approach requires the preparation of 5-10 minute topic presentations covering IAS issues such as buffer-overflow and the dissemination of the curriculum materials to the faculty so that it requires minimal preparation to insert IAS content into existing lectures.
3. Complete lectures: This approach is useful when remedial instruction must be inserted into an existing course for students that attended a course before a topic was integrated into the current perquisite. The creation of 1 hour stand-alone lectures on various topics also allows one to easily create seminar sessions to help lab and teaching assistants understand the changes to content of courses as they evolve.
4. Modules of instruction: We have found that some topic areas simply don't fit into a 1 hour format. For example, if one wanted to include digital forensics and media analysis in an operating systems class, one could insert a module on evidence gathering and chain of custody along with the technical aspects of media analysis. Several students commented that they never understood file systems until they dissected them using forensic tools.
5. Companion courses: This approach takes an existing 3 credit hour technical course (such as Operating Systems) and adds a 1 credit hour companion course that focuses on IAS issues as they relate to the topic of the 3 credit hour course.
6. Complete courses: This is the most common approach to adding content to a curriculum. We have found that great efficiency in presentation can be gained by looking at course outcomes of the curriculum as a whole and then refactoring topic coverage to incorporate fundamental concepts early. In one case we found that certain topics were being covered 3 times at an introduc-

tory level in upper division courses because they didn't share a common prerequisite and could be taken in different sequences. Putting introductions to operating systems concepts, databases, information assurance, networking, and system administration into a sophomore course freed 2-4 weeks of contact hours in each of our junior core courses. The additional time was used to include coverage of more advanced concepts.

In summary, we present the following. It is possible to integrate Information Assurance and Security concepts as a pervasive theme into an existing IT curriculum as is recommended by IT2005. We believe that the approaches we have used can be applied in other computing disciplines.

SIGITE and the CC 2005 Joint Task Force solicit feedback on the documents at http://www.acm.org/education/.

Acknowledgments

The authors would like to thank the ACM Education committee for their support of the IT2005 effort, especially Russ Shackleford, without whose financial support and encouragement the document would be years away from completion. We would also like to express appreciation to the NSA for funding the IAEGC (IAEGC 2006) program. Corey Schou's IAEGC lecture on helping students understand IAS in an hour was the genesis of the IAS approach in IT2005. The Brigham Young University authors would like to express appreciation to our colleagues and the administration of the School of Technology Brigham Young University, who covered our classes and found the funding for the time and travel our participation in the SIGITE curriculum committee required.

References

CERIAS web site (2006). http://cerias.purdue.edu/; retrieved June 20, 2006.

Dark, M., Ekstrom, J. & Lunt, B. (2006a). Experience Implementing IT2005 IAS Curriculum in Existing Programs, *Proceedings of the 10th Colloquium for Information Systems Security Education*, June 5-8, University of Maryland, MD, USA.

Dark, M., Ekstrom, J. & Lunt, B. (2006b). Implementation of Information Assurance and Security in Existing IT Curricula, *Proceedings of the 2006 ASEE Annual Conference & Exposition*, June 18-21, Chicago, IL; proceedings on CD-Rom (no page numbers).

Dark, M., Ekstrom, J. & Lunt, B. (2005). Integration of Information Assurance and Security into the IT2005 Model Curriculum, *Proceedings of the 2005 SIGITE Conference*, October 20-22, 2005, Newark, NJ; proceedings on CD-ROM (no page numbers).

Ekstrom, J. & Lunt, B. (2005). Integration of Information Assurance and Security into the IT2005 Model Curriculum, *Proceedings of the 9th Colloquium for Information Systems Security Education* 6-10 June, 2005, Georgia Tech Campus, Atlanta, Georgia, USA.

IAEGC (2005). Information Assurance Education Graduate Certificate, http://www.cerias.purdue.edu/iae Validated April 13, 2005.

Joint Task Force for Computing Curricula (2001). *Computing Curricula 2001, Computer Science Volume*, December 15, 2001, Copyright 2001, ACM/IEEE

Joint Task Force for Computing Curricula (2005). *Computing Curricula 2005: Overview Document*, http://www.acm.org/education/Overview_Draft_11-22-04.pdf retrieved June 20, 2006.

Machonachy, V., Schou, C., Ragsdale, D. & Welch , D. (2001). A model for Information Assurance: An Integrated Approach, *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point , NY, 5-6 June 2001.

National Research Council. (2000). How People Learn: Mind, Brain, Experience, School. National Academy Press.

National Security Agency (2006a). http://www.nsa.gov/ia/iaFAQ.cfm?MenuID=10#1, retrieved June 20, 2006

National Security Agency (2006b). http://www.cnss.gov/history.html, retrieved June 20, 2006

National Security Agency (2006c). http://www.nsa.gov/ia/academia/caeCriteria.cfm?MenuID=10.1.1.2, retrieved June 20, 2006

National Security Agency (2006d). Information Assurance Division; http://www.nsa.gov/ia/ retrieved June 20, 2006.

SIGITE Curriculum Committee (2005). *Computing Curriculum 2005, IT Volume*, http://www.acm.org/education/ curric_vols/IT_October_2005.pdf retrieved June 20, 2006

Appendix A

From IT2005 Mar 2005 Draft

The Information Technology Body of Knowledge

ITF. Information Technology Fundamentals (33 core)

ITF1. Pervasive Themes in IT (17)
ITF2. Organizational Issues (6)
ITF3. History of IT (3)
ITF4. IT and Its Related and Informing Disciplines (3)
ITF5. Application Domains (2)
ITF6. Applications of Math and Statistics to IT (2)

HCI. Human Computer Interaction (20 core hours)

HCI1. Human Factors (6)
HCI2. HCI Aspects of Application Domains (3)
HCI3. Human-Centered Evaluation (3)
HCI4. Developing Effective Interfaces (3)
HCI5. Accessibility (2)
HCI6. Emerging Technologies (2)
HCI7. Human-Centered Software (1)

IAS. Information Assurance and Security (23 core)

IAS1. Fundamental Aspects (3)
IAS2. Security Mechanisms (Countermeasures) (5)
IAS3. Operational Issues (3)
IAS4. Policy (3)
IAS5. Attacks (2)
IAS6. Security Domains (2)
IAS7. Forensics (1)
IAS8. Information States (1)
IAS9. Security Services (1)
IAS10. Threat Analysis Model (1)
IAS11. Vulnerabilities (1)

IM. Information Management (34 core hours)

IM1. IM Concepts and Fundamentals (8)
IM2. Database Query Languages (9)
IM3. Data Organization Architecture (7)
IM4. Data Modeling (6)
IM5. Managing the Database Environment (3)
IM6. Special-Purpose Databases (1)

IPT. Integrative Programming & Technologies (23 core)

IPT1. Intersystems Communications (5)
IPT2. Data Mapping and Exchange (4)
IPT3. Integrative Coding (4)
IPT4. Scripting Techniques (4)
IPT5. Software Security Practices (4)
IPT6. Miscellaneous Issues (1)
IPT7. Overview of programming languages (1)

NET. Networking (20 core hours)

NET1. Foundations of Networking (3).
NET2. Routing and Switching (8)
NET3. Physical Layer (6)
NET4. Security (2)
NET5. Application Areas (1)
NET6. Network Management

PF. Programming Fundamentals (38 core hours)

PF1. Fundamental Data Structures (10)
PF2. Fundamental Programming Constructs (9)
PF3. Object-Oriented Programming (9)
PF4. Algorithms and Problem-Solving (6)
PF5. Event-Driven Programming (3)
PF6. Recursion (1)

PT. Platform Technologies (14 core hours)

PT1. Operating Systems (10)
PT2. Architecture and Organization (3)
PT3. Computer Infrastructure (1)
PT4. Enterprise Deployment Software
PT5. Firmware
PT6. Hardware

SA. System Administration and Maintenance (11 core hours)

SA1. Operating Systems (4)
SA2. Applications (3)
SA3. Administrative Activities (2)
SA4. Administrative Domains (2)

SIA. System Integration and Architecture (21 core hours)

SIA1. Requirements (6)
SIA2. Acquisition/Sourcing (4)
SIA3. Integration (3)
SIA4. Project Management (3)
SIA5. Testing and QA (3)
SIA6. Organizational Context (1)
SIA7. Architecture (1)

SP. Social and Professional Issues (23 core hours)

SP1. Technical Writing for IT (5)
SP2. History of Computing (3)
SP3. Social Context of Computing (3)
SP4. Teamwork Concepts and Issues (3)
SP5. Intellectual Properties (2)
SP6. Legal Issues in Computing (2)
SP7. Organizational Context (2)
SP8. Professional and Ethical Issues and Responsibilities (2)
SP9. Privacy and Civil Liberties (1)

WS. Web Systems and Technologies (21 core hours)

WS1. Web Technologies (10)
WS2. Information Architecture (4)
WS3. Digital Media (3)
WS4. Web Development (3)
WS5. Vulnerabilities (1)
WS6. Social Software

Total Hours: 281

Appendix B

Brigham Young University Course Flow Chart