Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

The Need for Information Assurance Curriculum Standards

Carol Taylor, *Member, IEEE,* and Jim Alves-Foss, *Member, IEEE*

Abstract – In this paper we discuss the need for an Information Assurance (IA) curriculum standard for college-level IA programs. Existing IA standards emphasize professional training as opposed to education, and are not general enough for typical undergraduate programs. We present curriculum development efforts from colleges based on existing standards, which demonstrates the problems with these standards. We propose a process for the creation of a standardized IA curriculum that could serve as a model for college IA programs. The process for designing a standardized IA model is based on a successful curriculum design model from MIT.

I. INTRODUCTION

In 2005, computer security remains an unsolved problem that appears to be growing worse. Tumbleweed Communications, an e-mail security provider estimates that two-thirds of all e-mail is illegitimate traffic [1]. Botnets which consist of hacker controlled networks of 100's or 1000's of hosts are one of the fastest growing menaces on the Internet. These networks are capable of launching DDoS attacks, untraceable spam relays and widespread malware attacks [2]. SEI/CERT has stopped reporting incidents since they feel that widespread use of automated attack tools are so common that incident counts no longer provide meaningful information [3].

Proposed solutions to what appears to be an increasingly unmanageable problem are overwhelmingly technical. New security products continue to appear, promising to fix holes left behind by the last set of products. The Computing Research Association's (CRA) "Grand Challenges in Information Security and Assurance" workshop in 2003, identified four challenges including the elimination of epidemic style attacks, development of tools to construct large scale trustworthy systems, better quantitative risk management, and end user security that can be understood [4]. While security education is implicit in most of these grand challenges, education of current and future developers is not considered important enough to be one of the security challenges.

Education has been suggested as one way to reduce the risk from computer crimes. The security community, government and academia emphasize user education as a way for people to protect themselves from computer crime [5, 6, 7, 8]. However, security education for CS students or professionals is not generally recognized as a solution to cyber security problems. Recently, a few industrial groups have begun initiatives aimed at educating software professionals in order to improve the quality of software. In 2002, Microsoft, the largest producer of software shut down its operation for several weeks in order to train its work force in secure software development [5]. Another effort aimed at secure development is the recent creation of a task force to improve security across the software development lifecycle [9]. The task force, "Improving Security Across the Software Development Lifecycle" is comprised of both public and private security experts whose goal is to increase software security but also allow the benefits of software innovation [9]. One of their goals is to enhance the training and education of present and future developers in putting security at the heart of software design [9].

Strong security education programs have existed for many years in a select few universities [10, 11] and DOD supported educational institutions [12, 13]. In addition to these established programs, the NSA program to create college Centers of Academic Excellence (CAE) in Information Assurance Education (IAE) has designated 59 colleges in 27 states [14]. Yet, the majority of CS and IS programs in the US offer no courses in computer security or secure code development. While there are several reasons for the lack of security courses in CS programs, we believe one factor that compounds the problem is the lack of a standard college level IA curriculum.

The CISSE Conference begun in 1997 is one relatively recent effort to create a forum for security education [15]. While standards have been discussed at CISSE, no agreed upon standards have emerged as a result of the CISSE conferences. Other IA curriculum efforts include:

Carol Taylor, Post-doctoral fellow, University of Idaho
Jim Alves-Foss, Associate Professor, University of Idaho

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

- The Information Assurance Curriculum Development Project, a three year NSF funded program begun in 2001. Their goal was the production of an educational framework for both undergraduate and graduate Information Assurance programs [16]
- A model curriculum in Information Assurance developed by Kennesaw State University [17]
- A security curriculum development conference at Kennesaw State in 2004 [18]

The most common standards currently used to develop security curriculum are the NSTISSC 40XX Series of Infosec training standards [14][1]. Yet, for a university interested in developing an information assurance course or an entire curriculum, there is no single widely endorsed education standard that can serve as a guide. Based on our own and others experiences in IA course development, we believe there is a strong need for a college level IA curriculum model.

In this paper, we attempt to accomplish two goals. One is to present our experience at the University of Idaho in updating and expanding our information assurance courses. We examine the difficulties in designing a quality program in the absence of a general IA curriculum standard, which appears to be a problem common to other universities. The second goal is to outline a process based on a successful curriculum development model, the MIT CDIO model [19] that could lead to a standard IA college level curriculum. The purpose in developing a standard curriculum is that it could serve as a template for number of college institutions.

This section introduced the need for a standard college level curriculum model. Section two describes the current IA standards and other curriculum efforts. In Section three we describe the evolution of our security curriculum at the University of Idaho. Section four elaborates on the problem of non-existent IA standards while Section five describes the MIT CDIO model and proposes a solution for creating an IA curriculum standard using a CDIO-like process. We present our conclusions and recommendations in Section six.

II. IA STANDARDS AND CURRICULUM EFFORTS

In this section we provide an overview of the existing standards that are commonly used to develop IA curriculum for university programs. We also cover existing curriculum development projects and provide examples of several colleges that have tried to develop IA curriculum using the current standards.

a A. Information Assurance Standards

NSTISSI 4011

Currently, the most widely used standard in IA curriculum development is the NSTISSI Training standards, particularly, NSTISSI 4011. The NSTISSI Training standards were created to establish a set of topics and learning outcomes for industry information system security professionals [14]. The 4011 definition of an Infosec professional is:

> *Someone who is responsible for the security oversight or management of national security systems during all phases of the life cycle.*

The 4011 standard includes the seven areas listed by their suggested sequence order in Figure 1.

NSTISSI 4011 Seven Topic Areas

Communication Basics
|
Automated Information System Basics
|
Security Basics
|
NSTISS Basics
|
System Operating Environment
|
NSTISS Planning and Management
|
NSTISS Policies and Procedures

Figure 1. NSTISSI 4011

Under each area are lists of *Instructional Content* plus specific *Behavioral Outcomes* related to the *Instructional Content*.

In assessing 4011's suitability for college curriculum development, several problems were noted. Wording throughout the document is highly specific to government systems with many references to government automated information systems. Plus topic areas are unrelated to a general curriculum such as *NSTISS Basics* and *NSTISS Policies and Procedures*. Under these topic areas are many references to agency specific policies and contact personnel within agencies. While these topics may be related to training government security personnel, they don't apply to students in a college environment.

[1] We exclude commercial certification training standards since their goals are training and not education

For an institution to become an NSA approved Center of Academic Excellence, the college must undergo certification of their academic security program. Part of the certification process involves showing that their security curriculum teaches the necessary skills specified in the 4011 training standard plus at least one other NSTISSI 40XX standard. All topics in 4011 must map to an academic course even those that are not relevant to students.

ACM/IEEE 2001 Netcentric Computing

Within the ACM/IEEE 2001 curriculum, the Netcentric sub-topic covers material related to networking [20]. Nine topics are listed under the Netcentric specification two of which relate to computer security: Network Security and Network Management [20].

The ACM/IEEE curriculum is specifically designed for curriculum development. Topics are directly mapped into courses with suggested credit hours and learning outcomes. Yet, the suggested topics for network security, which is considered a core course, are not complete enough for a network security course. The content is heavily slanted towards cryptography without any practical security coverage. The practical issues related to network threats and defense mechanisms are included in the Network Management course, which is an elective [20].

While ACM/IEEE's Netcentric computing sub-topic is better suited to undergraduate education, it is not complete in its treatment of network security and makes no attempt to cover the entire spectrum of security education. Nowhere else within the 2001 ACM/IEEE curriculum guide is security mentioned [21].

Report on Information Assurance Curriculum Development

In 2001, NSF funded a three-year project whose objective was to develop a curriculum framework for undergraduate and graduate programs in Information Assurance [16]. The project goals were to identify broad areas of knowledge considered important to practicing professionals who graduate from college level programs. The output of the curriculum design effort was what should be taught (content) along with key learning outcomes or what the student knows and should be able to do (scope) [16].

The intent of the curriculum initiative was to provide a framework that would serve multiple purposes. Faculty could fill gaps in existing programs and develop new IA programs based on student learning outcomes. Employers would benefit from the initiative since they could see what IA graduates should know plus students could determine what they needed to know upon graduation from an IA program.

Outcomes from the initiative were a list of topics that should be covered and an associated indicator of depth of knowledge adapted from the standard Bloom taxonomy of cognitive knowledge[2]. Under the Bloom taxonomy, *Declarative* knowledge means a student knows that something is the case, *Application* knowledge uses learned material in new situations and *Synthesis* means to create new solutions from existing knowledge [16].

The Report's authors acknowledged that the report was preliminary and expected that further work would refine the document and add to the Bloom knowledge levels. Yet, no further work was ever published from this project or attempt made to generate a standard curriculum from this framework of IA topics.

Kennesaw State Draft Curriculum

One of the most complete proposed curriculums is from Kennesaw State University titled A Draft Model Curriculum for Programs of Study in Information Security and Assurance [17]. The authors both of whom hold CISSP security certifications from ISC^2, reviewed the available standards including ISO/IEC 17799, NSTISSI Training standards, NIST documents and the commercial certifications by ISC^2, SANS and others. Their draft proposed curriculum provides an excellent overview of these standards and certification procedures [17]. They based their curriculum on the Core Body of Knowledge needed for the CISSP certification and the NSTISSI training standards.

The Kennesaw State Draft Curriculum was developed as a general IA curriculum that could serve both IS and CS college-level undergraduate programs. This model document is complete in its recommendations for courses, learning outcomes, proficiency levels and even recommended labs to accompany the courses. However, examination of course content and focus suggests this curriculum is better suited for IS than CS programs. Also, the choice of a professional training standard, the CISSP certification as a basis of the program suggests more of a job training emphasis than a general college level curriculum.

B. Examples of IA Curriculum Design

Many colleges have developed IA programs without the benefit of a standard core body of knowledge. We include two studies that report on their attempts to develop college-level IA programs. Both colleges document the

[2] Refer to the NSF Report [16] for details on how the Bloom taxonomy was used to set proficiency levels

challenges they faced as they developed their IA programs.

The University of Wisconsin – Superior describe their experience in trying to design an IA curriculum for CS students in a liberal arts college [22]. They discuss the difficulty of meeting the NSTISSI Training Standards whose focus is vocational and includes specific low-level core competencies. The authors examined other curriculum models such as the NSF IA Project [16] and commercial IA training standards and found that none of them were suitable for undergraduate liberal arts education [22].

The second example is from a small university, Southern Oregon University (SOU), who similarly describe their experience in creating a BS degree in computer security and IA (CSIA) [23]. They used the 4011 training standard and then augmented the topics with outside material drawn from their university's strengths in criminology along with their own industry experience. Since SOU's intention was to become a future NSA CAE, using 4011 as a foundation made sense since their courses would have to map to the 4011 topics in order to qualify as a Center of Academic Excellence [23]. However, they mention that they tried but failed to find a peer institution with an undergraduate program that could serve as model.

III. IA CURRICULUM AT THE UNIVERSITY OF IDAHO

The University of Idaho is a land grant university of about 10,000 students. The computer science department has a strong program offering both undergraduate and graduate CS degrees at both the MS and PhD levels. Currently, we have about 300 undergraduate students and 238 MS and PhD students. Our department has 13 full-time faculty, who teach and conduct research. There are five faculty affiliated with the IA program plus two post-doctoral fellows that also teach and conduct research. In addition to our IA concentration, the CS department also has a strong program in bioinformatics and evolutionary computing plus expertise in software engineering.

A. Our IA Development Process

Information assurance curriculum development at the University of Idaho began in 1991 with the arrival of Dr. Jim Alves-Foss. Dr. Alves-Foss graduated from UC Davis with a specialty in computer security and became the first IA faculty at the University of Idaho. The first security course developed consisted of a combined upper division undergraduate and graduate course, in computer security that emphasized both theory and practical knowledge. The addition of a second IA faculty, Dr. Debra Frincke, in 1993 resulted in the creation of several more security courses, Network Security and a senior/graduate level seminar in Intrusion Detection.

These early courses were followed by a senior/graduate course in Survivable System Analysis, a seminar in Security Policies and a course in Exploit Techniques and Defense. Other CS faculty became interested in IA and assisted with the development and teaching of these courses. In 2004, several additional courses were added including Forensics analysis and a lower level general Security Course [24]. These courses evolved as the perceived need arose and as an outgrowth of faculty research interests.

During the period of our curriculum development effort, we became an NSA CAE/IAE [14] and also participated in the NSF Scholarship For Service (SFS) program [25]. The NSA program has certain curriculum requirements which must be met in order to qualify for program continuance. The NSA CAE/IAE designation is closely tied to the NSTISSI training standards especially 4011. In becoming an Academic Center of Excellence, the institution must demonstrate that their curriculum complies with the 4011 standard plus at least one other standard selected from the 4012 – 4015 documents [14]. The 4011 training standard was discussed in detail in Section two.

Certification verifies that the college teaches skills that cover each of the seven topic areas of 4011. Currently, our IA curriculum includes the classes shown in Figure 2.

Security Courses at University of Idaho

Undergraduate	
CS 204	Writing Secure Software
CS 336	Introduction to Information Assurance
CS 337	Advanced Information Assurance
CS 338	Network Security
CS 447	Computer Forensics
CS 449	System Survivability
Graduate	
CS 537	Advanced Information Assurance
CS 538	Network Security
CS 547	Computer Forensics
CS 549	System Survivability

Figure 2. University of Idaho IA Courses

In the next section, we assess how well our curriculum conforms to national standards and further critique the adequacy of the IA standards commonly used for curriculum development.

IV. UNIVERSITY OF IDAHO IA CURRICULUM MAP TO STANDARDS

In the course of applying for re-certification as a CAE, we mapped our curriculum to the NSTISSI 4011 standard [14]. Certification as a CAE/IAE provides us with evidence that our program satisfies the NSA/DHS criteria for IA education which demonstrates acceptance by a well-respected government program. However, recognition that our program meets government requirements for excellence does not verify our program's academic quality. In the absence of a universally accepted standard for IA curriculum like the ACM/IEEE curriculum standard [21], we lack a way to measure the academic quality of our IA program.

A. Critique of IA Standards

The main standard used to develop our curriculum was NSTISSI 4011 [14]. The motivation behind mapping our courses to 4011 included our desire to continue as a Center of Excellence and the lack of any other obvious choice. Because 4011 is a required standard for institutions wishing to become CAE's it exerts a strong influence over national IA college-level curriculum. Yet, as previously stated, the 4011 standard has some serious drawbacks as a curriculum model for higher education.

NSTISSI 4011 was developed in 1994 as a training standard for security professionals [22]. A training standard does not necessarily endorse the same skills and qualities that are valued for higher education. The differences between IA training and college level education were recently discussed by Bishop and Frincke [26]. They noted that the primary differences between domain specific certification by professional organizations and academic education is that the focus of professional certification is on mastering a particular body of knowledge while education emphasizes basic skills and reasoning abilities

Faculty from Florida State University, one of the original NSA CAE's, describe goals for students in their IA programs which emphasizes abstract thinking and problem solving. They believe these learning outcomes are important so that students can handle today's complex security problems [27]. They further state that while hands-on training is valuable, abstraction is learned by discussion, modeling, proof of concept and mentoring activities [27].

The main problem with using NSTISSI 4011 as a guide to college level curriculum development is the fact that 4011 really is a training standard and doesn't go far enough in serving as a model that can be adopted by college programs. There are educational objectives and outcomes that go beyond specific IA training goals that should be incorporated into a model curriculum standard. General outcomes desirable from a college level educational program of study include communication skills both written and oral, problem solving, critical thinking, and interpersonal skills [28]. Ideally, recommendations on course sequencing or integration with existing programs would be included in a recommended IA course of study.

In trying to assess the quality of our IA courses, several non-IA specific standards were considered such as the ACM/IEEE 2001 curriculum standard [21] and the ABET 2000 accreditation standards [29]. The ACM/IEEE standard discusses security issues in their Netcentric Computing (NC) subject area [20]. As discussed in Section two, two out of the nine sub-topics, Network Security and Network Management outline topics and learning outcomes directly related to network security. The recommended topics include cryptography, authentication, digital signatures, network threats and defenses such as firewalls and recovery strategies. Our courses covered all of the topics in the Netcentric subject area. The ABET accreditation standard has no specific security requirements [29].

V. A MODEL FOR IA CURRICULUM

The problem of how to develop quality curriculum for higher education is not unique to IA education. A number of general educational resources can serve as a starting point when designing curriculum [28, 30]. Yet, designing a standard core curriculum that can serve as a guide for any four year institution is different than producing a specific college program. As such, we need a process that produces a general IA curriculum that can be customized to meet individual program needs. A search for successful models for curriculum design from other disciplines yielded a process model that has already proven successful, the CDIO Syllabus project from MIT [19].

The focus of the CDIO curriculum effort is to reform the Aeronautical undergraduate engineering program at MIT. The CDIO Syllabus effort is unique in that it not only produced a thorough requirements document for undergraduate engineering education, but also produced a well-documented, repeatable process for creating curriculum for any engineering-related discipline [19].

A. CDIO Model Syllabus

The CDIO model begins with an agreed upon goals statement that captures the knowledge, skills and attributes of a university educated engineering student. This statement is then iteratively refined into successive levels of learning objectives. The CDIO goals statement is [19]:

> Conceive-Design-Implement-Operate
> complex value-added engineering systems
> in a modern team-based environment

From this statement a complete set of topics is derived that facilitate the implementation and assessment of the overall goal. The high-level topics represent three knowledge areas shown in Figure 3.

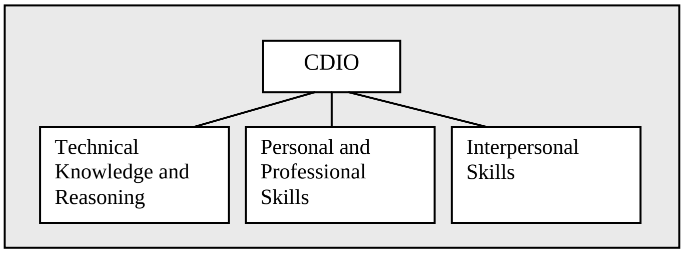
CDIO
Technical Knowledge and Reasoning
Personal and Professional Skills
Interpersonal Skills

Figure 3. CDIO engineering knowledge areas

The reasoning behind this division is that engineering students should know technical, professional and interpersonal skills in order to become fully trained individuals. Each of these three areas is further broken down into specific objectives that further support the high level goal. For example, the high level goal of Personal and Professional Skills and attributes becomes:

> 2.1 Engineering reasoning and problem solving
> 2.2 Knowledge discovery
> 2.3 Personal skills and attributes
> 2.4 System thinking
> 2.5 Professional skills and attitudes

Each of these topics are iteratively refined into successive set of more detailed objectives until a set of teachable and assessable skills is reached [19].

B. CDIO Process

Creating the CDIO Syllabus was accomplished by following a process that was documented and repeatable so that the Syllabus could be updated and revised. The process is outlined below [19]:

1. Interview focus groups of MIT faculty, current MIT students, industry leaders and senior academics from other universities
   All groups were asked,
   > *"What in detail is the set of knowledge, skills and attitudes that a graduating engineer should posses?"*
2. Results are organized into a preliminary draft
3. Standards such as the ABET EC 2000 and Boeing's engineering requirements are used to augment the group suggestions
4. A draft is distributed to another set of groups including industry leaders, MIT faculty, alumni and other academics. Draft comments are incorporated.
5. Proficiency levels for learning objectives are determined based on a 5 point activity scale and sent to professionals, faculty, industry and alumni
6. Feedback from the proficiency survey is tabulated and major discrepancies between group responses are resolved

C. An IA CDIO Process

The CDIO Syllabus project details a process for defining an engineering curriculum based on specific student outcomes. Curriculum development begins with a general goals statement that is then refined into learning objectives that are detailed enough to generate specific course objectives and assessments.

We believe the CDIO process can serve as a model for developing an IA college level curriculum. Steps in an IA CDIO process include:

1. Interview Groups
   - ➢ Conduct interviews with stakeholder groups: Government, faculty, students and industry representatives from a range of different sized programs
   - ➢ Ask the question,
     "What in detail is the set of knowledge, skills and attitudes that a graduate from an IA program should posses?"

2. Develop Draft
   - ➢ Distill answers from interviews into one or several high level goals statements that can be further refined into learning objectives
   - ➢ Augment the survey answers with topic material from relevant security standards

3. Review Draft
   - ➢ Pass out draft to industry, faculty, students and alumni to get feedback
   - ➢ Incorporate their comments
4. Set Proficiency Levels
   - ➢ Determine proficiency levels for each learning objective

- Get feedback from all the previous surveyed groups on the proficiency levels

We believe there would be multiple benefits to using an IA CDIO model to develop a standardized curriculum. All groups with a vested interest in information assurance education would be represented which would more likely lead to consensus and adoption than if a single university, government or industry group proposed their own curriculum. The quality of the curriculum will likely be better for having been widely reviewed. A final benefit is that the curriculum ultimately developed from the list of topics and learning objectives is not dictated by the IA CDIO process. Individual institutions are free to create their own courses and map them to the IA learning objectives.

D. Potential Difficulties

Because the CDIO model was developed for a specific sub-discipline of engineering, Aeronautical Engineering, there was consensus between the groups surveyed. For the IA field, which is broader and still actively evolving, there will more likely be disagreement between the groups surveyed. Thus, resolving dissention could be a significant effort. Also, we anticipate that it is unlikely that a one-size-fits-all curriculum model for IA undergraduate education will be sufficient. There may need to be a separate curriculum model for IS and CS where there are fundamental program differences as discussed in the latest ACM computing curriculum report [31].

VI. CONCLUSION AND RECOMMENDATIONS

In this paper we presented a critique of IA standards for college curriculum development along with a suggested process model for creating a standard core IA curriculum. We discussed some problems with the IA standards for college level curriculum development which emphasize training as opposed to education. We then used our experience along with other colleges in creating security courses without the benefit of a standard IA curriculum. A potential model was outline for undergraduate IA curriculum development based on the engineering CDIO model from MIT. In our opinion, this model offers the potential benefit of consensus from many groups interested in Security education. Using an IA CDIO model, would lead to a general curriculum that could eventually be standardized.

Ultimately the goal in developing a standard, widely endorsed IA curriculum is to provide guidance for universities that want to implement their own IA program. In order to achieve this goal, the curriculum model will need to be detailed enough so that courses and assessments can be created from the model.

It is our belief that security education is a critical component in safeguarding our systems by creating developers and IT workers who are aware of the consequences of insecure code. The current “deploy and patch” mentality of commercial software vendors is not a viable solution for a sustainable future that requires safe, trustworthy systems. Currently, some government and industry groups recognize the importance of IA education but until education becomes one of the acknowledged “grand challenges” of the security community it is doubtful that system quality will significantly improve.

VII. REFERENCES

[1] Saita, A. “Ripe for Harvest”, Information Security, Vol. 8,3, March 2005.

[2] Dittrich, D. “Invasion Force”, Information Security, Vol. 8,3, March 2005.

[3] Landwehr, C. E., “Changing the Puzzle Pieces”, IEEE Security & Privacy, Vol. 3,1, Jan/Feb 2005

[4] CRA, “ Grand Challenges in Information Security and Assurance”, http://www.cra.org/Activities/grand.challenges/security/home.html, 2003.

[5] Howard, M. and B. LeBlanc, “Writing Secure Code”, Redmond, WA, Microsoft Press, 2003.

[6] CERT. “Improve Security”, http://www.cert.org/nav/index_green.html

[7] NIST. “Computer Security Division”, http://www.csrc.nist.gov/

[8] Skoudis, E. “Counter Hack”, Prentice Hall, NJ, 2002

[9] US National Cyber Partnership. “Improving Security Across the Software Development Lifecycle”, http://www.cyberpartnership.org/SDLCFULL.pdf, 2004

[10]CERIAS. Center for Education and Research in Information Assurance and Security, http://www.cerias.purdue.edu

[11] Seclab. UC Davis, Seclab. http://seclab.ucdavis.edu

[12] Naval Postgraduate School. http://www.nps.navy.mil

[13] Air Force Institute of Technology. http://www.afit.edu/af_info/af_info.cfm

[14] NSA. "National IA Education and Training Program", http://www.nsa.gov/ia/academia/cnstesstandards.cfm

[15] CISSE. "Colloquium for Information Systems Security Education", http://www.nisse.org

[16] Dark, M. and J. Davis. "Report on Information Assurance Curriculum Development", CERIAS, Purdue University, 2002.

[17] Whitman, M.E. and M.J. Mattord. "A Draft Model Curriculum for Program of Study in Information Security and Assurance", http://www.course.com/corners/security/KennesawinfoSecCurriculumModel.pdf

[18] KSU. "Curriculum Conference", http://infosec.kennesaw.edu/InfosecCD2004/index.shtml

[19] Bankel, J. et al. "The CDIO Syllabus: A Comparative Study of Expected Student Proficiency", http://www.mit.edu/aeroastro/www/cdio/cdiodocuments/CDIO.pdf

[20] ACM/IEEE. "Netcentric Computing", http://www.computer.org/education/cc2001/final/nc.htm

[21] ACM/IEEE. "Computing Curricula 2001 Computer Science Volume, December 15, 2001", http://www.sigcse.org/cc2001

[22] Piotrowski, V. "Information Association Curriculum and Certifications", 36th Annual Midwest Instruction and Computing Symposium, MICS, 2003.

[23] Bacon, T. and R. Tikehar. "Experience with Developing a Computer Security Information Assurance Curriculum", Journal of Computing Sciences in Colleges, Vol. 18,4, April 2003.

[24] CSDS. "CS Based IA Curriculum", http://www.csds.uidaho.edu/IA/IAStudy.htm

[25] NSF. "CCLI Program", http://www.ehr.nsf.gov/EHR/DUE/programs/ccli/default.asp

[26] Bishop, M. and D. Frincke. "Academic Degrees and Professional Certification", IEEE Security & Privacy, Vol. 2, 6, 2004.

[27] Yasinac, A. and M. Burmester. "Centers of Academic Excellence: A Case Study", IEEE Security & Privacy, Vol. 3, 1, 2005.

[28] Diamond, R. M., "Designing and Assessing Courses and Curricula: A Practical Guide", Jossey-Bass Pub., S.F., 1998.

[29] ABET. "Accreditation Criteria", http://www.abet.org/criteria_cac.html

[30] Fink, L. D. "A Self Directed Guide to Designing Courses for Significant Learning", University of Oklahoma, http://www.byu.edu/fc/pages/tchlrnpages/Fink/Fink_Article.pdf

[31] ACM/AIS/IEEE. "Computing Curricula Overview Report", http://www.acm.org/education/overview_Draft_11-22-04.pdf, 2004