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

Information Assurance Educational Outreach: Initiatives at the Software Engineering Institute

Carol A. Sledge

Abstract – The Software Engineering Institute[1] (SEI) seeks to transition courseware, materials and a survivability and information assurance curriculum to various departments at institutions of higher education, with a particular focus on Minority Serving Institutions (MSIs) and community colleges. Rather than build an infrastructure to accomplish this, the SEI utilizes partnerships which leverage the strengths of the SEI and the strengths of the partner educational institutions and builds upon existing trusted relationships and infrastructure, and sustains the incorporation of new and evolving materials. Leveraging other complementary programs, events and organizations broadens the offering and makes it more cost effective to all parties concerned. Over the past three years, the SEI has developed a four-pronged approach for its educational outreach in information assurance, with the goal of increasing the educational IA capacity.

Index terms – information assurance education, information security education, regional collaborative cluster, capacity building

I. Background

From the inception of the Software Engineering Institute until 1995, the SEI's Education Program defined Master's and Undergraduate Software Engineering Curricula, created materials and courses in those areas, and transitioned same to the academic and continuing education communities. Successful transition meant the educational institution had the capacity to initially incorporate those software engineering materials and courseware, as appropriate, into their courses and curricula, and, over time, to continue to refine and expand the materials and courseware to better reflect that institution's educational interests and strengths, and to incorporate changing technology. In other words, the SEI's materials and courseware provided a 'jumpstart', enabling the institution to more quickly incorporate and offer software engineering subjects. While materials and courseware might be shared among faculty at that particular institution, unless a faculty member moved to a different institution and used derivative materials at that new institution, the transition was basically 1:1, from the SEI to the original institution, and on a course by course basis.

A decade later, through its Networked Systems Survivability (NSS) Program, the SEI is again engaged in the transition of curriculum, courseware and materials to the greater educational community, this time in the area of information assurance and with an updated approach for transition and capacity building. Just as information assurance issues pervade all aspects of every day life, information assurance-related topics are not limited to computer science, information science, and software engineering disciplines, but are also applicable in the business administration and management areas, for example. Information assurance education needs to address not only the individuals who will comprise the workforce of tomorrow, but also individuals such as system and network administrators in today's workforce. In particular, this education should complement, not compete with existing information security training. Within this context, over the past three years the SEI has developed a four-pronged approach for its educational outreach in information assurance with the goal of increasing the educational IA capacity.

II. Approach

The four-pronged approach involves

- working with higher education institutions (primarily undergraduate and graduate), with a focus on minority serving institutions, through direct educational outreach,
- creating regional information assurance collaborative clusters (colleges, universities and community colleges),
- creating a survivability and information assurance curriculum, initially for community colleges, and
- working with National Science Foundation (NSF) Advanced Technological Education (ATE) projects and centers to reach community colleges, colleges and universities.

The various aspects of the approach are not necessarily independent of one another, and indeed, in the future, the interaction and interplay between our key partner educational institutions serves to multiply the amount of educational materials available and the range of the

Carol A. Sledge is a Senior Member of the Technical Staff at the Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213

[1] The SEI is a federally funded research and development center sponsored by the U.S. Department of and operated by Carnegie Mellon University.

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

transition activity. Three fundamental precepts inherent in this approach are leveraging of exiting efforts, development of complementary educational materials, and the success of the SEI is dependent upon the success of its educational partners. Each of the four aspects of the approach will be discussed, in the order in which they were implemented. For the most part, later aspects build upon former aspects.

A. Direct Educational Outreach

Since 2002, the NSS Program has had an educational outreach program, targeting primarily Historically Black Colleges and Universities (HBCUs) and Hispanic Serving Institutions (HSIs), both of which fall under the larger category of Minority Serving Institutions (MSIs). Initially we sought computer and/or information science departments with the following characteristics:

- desire by the department to offer or to enhance their offerings with information security topics
- multiple faculty with an interest in this area
- long-range goal of offering information security/information assurance courses leading to a concentration/certificate program/option at the undergraduate or graduate level or a professional degree (e.g. Masters)
- strong support by the Departmental Chairperson
- strong support from the Dean of their school, and
- a desire to work with us to transition information security materials to their particular academic educational environment

The NSS Program offers a variety of short training courses in information security and assurance, aimed primarily at the professional workforce, either to enhance the skills and knowledge they have, or to learn new skills and knowledge. As stated, these are training courses, not necessarily in the form or format for an academic offering in an institution of higher education. However, if a faculty member already had the capacity to understand these training materials, could adapt and adopt this courseware for use in their courses and curriculum (academic-use), and was willing to share the derivative educational materials, we provided that faculty member with the courseware. Like the SEI's software engineering education model, this provided the faculty member with a 'jumpstart' to introduce new or additional information security topics, labs or courses into the curriculum, as appropriate.

While this helped some faculty and some departments, it did not help those departments and faculty who met our criteria, but who did not yet have the necessary capabilities and capacity to take advantage of our existing materials. Leveraging our involvement with an NSF capacity building program provided the opportunity to enlarge the set of faculty with the capacity to teach information security topics.

Since 2002, members of the NSS Program at the SEI have helped select faculty and have participated yearly in a month-long, NSF-funded Information Assurance (IA) Capacity Building Program (IACBP) at Carnegie Mellon University. Initially targeting computer and information science faculty at minority serving institutions, the IACBP helps faculty better understand information assurance/security topics, provides additional course material and offers networking opportunities with other faculty and researchers. Not only does this provide faculty with the opportunity to create short and long term plans for the incorporation of information security/assurance topics and courses into their curriculum, as appropriate, but the faculty at a particular capacity building program offering work together with faculty from other schools that share their same interests, and in a number of cases, are willing to share their own information security materials or to work collaboratively to create new materials. Finally, Carnegie Mellon's IACBP supports multiple faculty from the same educational institution over a period of two years to help build a critical mass at that department to better insure the completion of their short- and longer-term plans for the incorporation of information security into their curriculum. This past year, the IACBP added faculty from business departments that have a strong information systems component and thus an interest in enhancing the information assurance coverage in their curricula.

A side benefit of the month-long program at Carnegie Mellon is that it allows us to meet with the faculty participants on a regular basis, outside of the program hours, to enhance and evolve plans for the transition of additional NSS materials and courseware, and to also introduce and facilitate discussions between the faculty and other NSS or SEI members who are working in areas of interest to the faculty.

While successful, the NSS Program's direct educational outreach and Carnegie Mellon's IACBP program can only reach a limited number of faculty and schools each year. How to leverage and build upon the IACBP and the NSS Program's initial educational outreach? Part of the answer lay in the creation of Regional Collaborative Clusters.

B. Regional Collaborative Clusters

A Regional Collaborative Cluster (RCC) is a collection of educational institutions in a particular geographic region that at some level

- share a common vision and target student population
- have cooperated in the past, or can reasonably be expected to cooperate
- have a desire to incorporate or expand their information assurance content

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

- are within a day's drive of one another

At the heart of the Regional Collaborative Cluster is the hub educational transition partner. Qualities of a successful hub educational transition partner include the:

- capacity to understand, adapt, refine and incorporate Information Assurance materials and courseware into existing courses and curricula
- support by the educational institution to accomplish the above
- active leadership and commitment by a faculty member respected by the community
- existence of trusted relationships with other Computer Science, Information Science, Software Engineering, or Business (Administration) Departments in the immediate geographical region and beyond
- commitment to advance the state of Information Assurance education in the region through the sharing of materials and courseware, facilitation of workshops and symposia, etc.
- ability to leverage other complementary relationships, grants and activities, and
- a somewhat central location with respect to the other educational institutions in the region to reduce travel time to workshops, symposia and other events.

This RCC model leverages the existing, trusted working relationships of the hub educational transition partner with other Computer Science, Information Science or Business Departments to help create an infrastructure (the Regional Collaborative Cluster) capable of transitioning information assurance concepts, materials and courseware through workshops, symposia, etc. to additional educational institutions to increase the IA educational capacity in that region.

The NSS Program and the SEI provide the hub educational transition partner with IA materials and courseware, SEI and Department of Homeland Security speakers for a kick-off (and a second) regional IA symposium, and, in certain cases, opportunity for free seats in SEI and NSS public courses, other SEI materials and courseware (as appropriate), entrées into other Carnegie Mellon University outreach programs, etc. The hub educational transition partner adapts, refines and incorporates the IA materials and courseware as appropriate to their particular environment and curriculum; shares the adapted and enhanced materials, courseware and experience with other academic educational institutions; sponsors and solicits attendees for the kick-off (and a follow-on) IA symposium (again leveraging its existing relationships); and hosts other IA-related workshops. The hub educational transition partner completely takes over responsibility for the regional IA symposium in the third and subsequent years.

The partnership between the SEI and the hub educational institution, and through its efforts, the Regional Collaborative Cluster, is ongoing: the better to sustain and enhance the IA educational capacity in that region. Whenever possible, both the hub educational transition partner and the SEI seek to leverage other complementary programs and efforts (such as the Carnegie Mellon University Information Assurance Capacity Building Program). The purpose is not to compete with other opportunities to enhance and improve educational IA capacity, but to build upon them.

The RCC concept supports our second-level transition of information security and assurance materials, courseware, etc. to the surrounding educational institutions through the hub educational transition partner. Our goal is to create a self-sustaining cluster of schools that continue to enhance and adapt materials to their particular curricula, and share those materials with faculty and colleges and universities.

The initial, prototype RCC, the Mid-Atlantic Regional Collaborative Cluster, with Hampton University as the hub educational partner was established in 2003 with Computer Science Department Chairman, Robert Willis, Jr., as our key collaborator and co-developer of our prototype offering. Willis and other members of his department had participated in the IACBP. The Mid-Atlantic RCC was based on Hampton University's and, in particular, Willis' existing relationships with Computer Science and Information Science Departments in HBCU's within a half-day's drive of Hampton. It encompasses 18 HBCU's in four states and the District of Columbia. Details about the formation of this prototype RCC, the initial successful kick-off IA Symposium on February 28, 2004, and other workshops held by Hampton University can be found in Sledge and Willis [1]. The Second Annual Hampton IA Symposium was held on April 2, 2005.

Two additional RCCs have been established, both targeting HSIs. The first focuses on California State University campuses and community colleges in southern California with California State Polytechnic University, Pomona (Cal Poly Pomona) and neighboring Mt. San Antonio Community College (Mt. SAC) of Walnut, CA as the hub educational transition partners. The second focuses on southern and coastal Texas with Texas A&M, Corpus Christi (TAMU-CC) as the hub educational transition partner.

Dan Manson of Cal Poly Pomona's College of Business Administration and John Blyzka of Mt. SAC's Computer Information Systems Department are our primary collaborators for the Southern California RCC, while John Fernandez and Mario Garcia of the Department of Computer and Mathematical Sciences at TAMU-CC are our

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

primary collaborators for the Southern Texas RCC. Like Hampton University, these faculty members from Cal Poly Pomona, Mt. SAC and TAMU-CC participated in the IACBP at Carnegie Mellon.

Although the three established RCCs share similarities, the RCCs and their hub educational transition partners also exhibit differences, which reflect not only the other programs that are being leveraged at these hub partners, but also the goals these partners have for the educational institutions in their region and for their own programs. Information on the activities of the hub educational partners can be found in Thomas [2].

For example, TAMU-CC is working to build capacity at community colleges and universities in Texas, initially with those at HSIs. In the future TAMU-CC also hopes to build capacity at Mexican universities with which it has relationships. The Department of Computer and Mathematical Sciences is starting a new option in information assurance for graduate students. TAMU-CC held its very successful First Annual IA Symposium on January 29, 2005, with the Second Annual scheduled for January 28, 2006. Mario Garcia is to spend the summer of 2005 at the SEI working with members of the NSS Program in areas of mutual interest and will then work to transition the knowledge and experience gained to TAMU-CC faculty and other faculty within its RCC.

Cal Poly Pomona now offers a Masters in Information Assurance and a new program, Professional MBA in Information Assurance, is under discussion. Additionally, certificate programs in IA with Mt. SAC and California State University, Los Angeles (Cal State Los Angeles) are under discussion. Cal Poly Pomona and Mt. SAC held their very successful first IA Symposium on December 11, 2004, with their follow-on IA Symposium to be held on December 10, 2005. In March 2005 Cal Poly Pomona hosted an Information Assurance curriculum development meeting. Faculty from four schools participating in a Title V Department of Education Grant titled " Improving Access to Information Systems at Hispanic-Serving Institutions: A Cooperative Arrangement" (California State University, San Bernardino, Cal State Los Angeles, Cal Poly Pomona and Mt. San Antonio Community College) attended, with additional faculty from other California State Universities. Cal Poly Pomona has also submitted, with co-principle investigators from Mt. SAC, an NSF Federal Cyber Scholarship for Service Capacity Building grant proposal entitled “A Regional Collaborative Cluster: Development Dissemination and Adaptation of Information Assurance Survivability Curriculum.”

C. Survivability an Information Assurance Curriculum

Today’s professional system and network administrators are increasingly challenged to make computer and network security a greater part of their already overflowing set of daily activities. Primarily through a Congressional earmark and working with the National Guard Bureau, the SEI has designed and is completing development of a three-course curriculum in survivability and information assurance (SIA). This is the curriculum referenced in the Cal Poly Pomona/Mt. SAC grant proposal.

The SIA curriculum is designed to teach system and network administrators about information assurance as well as a way to integrate IA into their routine tasks. They need a way to think about IA/security issues and a set of skills to help them integrate security policy, practices, and technologies into their operational infrastructure.

In addition, survivability – which we define as the capability of a system to fulfill its mission and provide essential services in the presence of attacks, accidents and failures, and to recover full services in a timely manner (Lipson and Fisher [3]) – is a relatively new responsibility for the entire organization, including system and network administrators. System and network administrators need to know their role and how to achieve the goals of survivability.

The SIA curriculum is based upon 10 principles that are emphasized throughout each course. These principles form a foundation that extends beyond any specific technology or implementation. Technology changes over time and this curriculum provides the student with a basis for assessing new technologies as they become available. While specific technologies are used in labs and assignments, these principles embodied in the curriculum are the key to meeting the curriculum goals.

Since the initial target students are experienced (2 years) system or network administrators, community colleges will be the first educational institutions to implement the curriculum. Subsequent versions of the curriculum will add material and courses to (initially) remove the experience requirement, and (later) to extend the curriculum.

As with our other approaches, the SEI seeks to build upon existing trusted relationships and infrastructure and to leverage other programs in getting this SIA curriculum to community colleges (and other colleges and universities). One avenue is to work with NSF ATE Centers and Projects.

D. Working with NSF ATE Projects and Centers

An NSF Regional Center for Systems Security and Information Assurance (CSSIA), based at Moraine Valley Community College in Palos Hills, IL, is the first comprehensive IT security center in the Midwest, according to Erich Spengler, its director. The center itself includes seven partner educational institutions and was established to address the needs for IT security professionals by increasing faculty expertise and higher education training programs in IT security and data assurance. The center offers training programs to community colleges and university faculty across the Midwest. As of Summer 2004,

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

over 75 schools were collaborating together to participate in developing quality IT Security programs and courses. The SEI has an existing relationship with CSSIA, and upon completion of the development of the SIA curriculum later this year, the SEI will transition those courses to CSSIA for adaptation and dissemination to interested CSSIA partners for academic-use.

Cal Poly Pomona and Mt. SAC are currently completing the second year of a three year NSF ATE Project Grant to develop a Regional Information Systems Security Center. They will soon begin work on a NSF ATE Regional IA Center grant with Cal State Los Angeles, other California State Universities and other community colleges in their region. This Regional Information Systems Security Center currently provides a means to disseminate, where appropriate, materials adapted from current SEI materials, and the proposed Regional IA center will provide a means to disseminate the SIA curriculum, again as adapted by Cal Poly Pomona and Mt. SAC.

III. Other Leverage Points

Through our relationships with faculty at Cal State Los Angeles and Cal Poly Pomona, we were able to present our NSS educational outreach programs and our Survivability and Information Assurance Curriculum to the Computer Science/Information Science/Software Engineering Discipline Council, comprised of Department heads in those disciplines from the 23 California State University campuses, and we have begun working with a number of those departments. Additional opportunities to share information and materials are available to the Discipline Council members through the Southern California RCC. We also look forward, as appropriate, to potentially leverage the Discipline Council's work with articulation programs with California community colleges. As Cal Poly Pomona and Mt. SAC define and implement their two plus two business degree in information assurance, another mechanism for transition of our (adapted) information assurance materials will be implemented. The SEI helps fuel the already existing collaboration between this university and this community college, and we support the extension of their strong collaborative model to other institutions.

The SEI has begun to work with a senior representative of the Hispanic Association of Colleges and Universities (HACU) to help raise awareness of Hispanic serving colleges and universities within the existing Regional Collaborative Clusters and to actively support the Regional IA Symposia (TAMU-CC). In addition, working together, we hope to identify not only additional schools and faculty with whom we can transition information assurance materials and identify potential hub education partners, but also to identify additional funding opportunities for those HSIs to support collaborative faculty development in information assurance and the incorporation of information assurance topics and courses in their curricula.

Finally, although in some cases our relationships with our hub educational partners are less than 18 months old, we can look forward in the not-too-distant future to the ultimate leverage: those hub educational partners working together and sharing derivative and enhanced materials they have adapted from our materials. We believe Dan Manson of Cal Poly Pomona and Erich Spengler of CSSIA will be among the first to find mutually beneficial sharing opportunities.

IV. Summary

Through its Networked Systems Survivability (NSS) Program, the SEI transitions information security and information assurance materials, courseware and an SIA curriculum to the greater academic educational community. Just as information assurance issues pervade all aspects of every day life, information assurance-related topics are not limited to computer science, information science, and software engineering disciplines, but are also applicable, for example, in the business administration and management areas. Information assurance education needs to address not only the individuals who will comprise the workforce of tomorrow, but also individuals such as system and network administrators in today's workforce. In particular, this education should complement, not compete with existing information security training. Within this context, over the past three years the SEI has developed a four-pronged approach for its educational outreach in information assurance with the goal of increasing the IA educational capacity.

The four-pronged approach involves

- direct educational outreach to faculty and departments in undergraduate and graduate programs,
- creating regional information assurance collaborative clusters
- creating a survivability and information assurance curriculum, initially for community colleges, and
- working with NSF ATE centers and projects to reach community colleges, colleges and universities.

While a 1:1 approach can transition materials, it is not the most efficient. By building upon existing trusted relationships and infrastructure, we can effectively extend our reach. One way to do this is to work with a hub educational transition partner, who is our key collaborator in creating, building and sustaining an IA Regional Collaborative Cluster. Leveraging their strengths and our strengths we work together to increase the number of information security topics and courses in the curricula of the participating schools in the RCC. Our goal is to create a self-sustaining cluster of schools that continue to enhance

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

and adapt materials to their particular curricula, and share those materials with other faculty and colleges and universities.

To address the needs of system and network administrators, we have designed and are completing development of a three-course curriculum in survivability and information assurance. These courses will be offered through community colleges, and will be adapted for use in undergraduate programs. One avenue for transition to community colleges will be to work through and leverage the work being done by CSSIA, an NSF ATE center, one of our key educational partners.

One of our goals is for our various hub academic educational partners to adapt, adopt and expand what we provide to those educational institutions within their various regions. Ultimately, we hope these hub educational partners will work with one another to leverage what they individually have developed. We seek to complement, not compete with other programs. Leveraging other complementary programs, events and organizations broadens the educational offering and makes it more cost effective to all parties concerned. Finally, we judge our success by the success of our education transition partners.

V. REFERENCES

[1] Sledge, Carol A. and Robert Willis, Jr. "Regional Collaborative Clusters: Building on Trusted Relationships to Increase IA Capacity." *Proceedings of the May 2004 Association of Computer and Information Science Engineering Departments at Minority Institutions (ADMI) Symposium*.

[2] Thomas, Bill. "University Hubs Help SEI Spread Information Assurance Curricula and Methods," *news@sei*, Volume 8, Number 1, pp. 8-9. Pittsburgh, PA, 2005.

[3] Lipson, Howard and David Fisher. "Survivability – A New Technical and Business Perspective on Security." *Proceedings of the 1999 New Security Paradigms Workshop*. Association for Computing Machinery. New York, 1999.

ISBN 1-933510-99-4/05/$15.00