Building Information Assurance Educational Capacity: Pilot Efforts to Date

Carol A. Sledge, Ph.D.

September 2005

SPECIAL REPORT
CMU/SEI-2005-SR-009

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Building Information Assurance Educational Capacity: Pilot Efforts to Date

CMU/SEI-2005-SR-009

Carol A. Sledge, Ph.D.

September 2005

CERT® Program

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

Abstract ..... **iii**

1 Introduction **1**
1.1 Prior Educational Initiatives at the SEI 1

2 Current Approach **3**
2.1 Direct Educational Outreach 3
2.2 Regional Collaborative Clusters 5
2.3 Survivability and Information Assurance Curriculum 9
2.4 Working with NSF ATE Projects and Centers 10
2.5 Leveraging State University Systems 11

3 Other Leverage Points **13**
3.1 Cross Departmental/Cross College 13
3.2 Associations 13
3.3 Within Carnegie Mellon University 14
3.4 Between Major Educational Partners 14

4 Future Work **15**
4.1 Future RCCs 15
4.2 New CERT Technology 15

5 Summary **17**

Appendix A Mid-Atlantic Regional Collaborative Cluster **19**

Appendix B West Coast Regional Collaborative Cluster **21**

Appendix C: Texas Regional Collaborative Cluster **23**

Appendix D Proposed Southern Regional Collaborative Cluster; Targeted HUCU Institutions (AL, TN, MS) **25**

References **27**

Abstract

This report describes efforts by the Software Engineering Institute (SEI) to increase the capacity of institutions of higher education to offer information assurance (IA) and information security (IS) courses, to expand existing IA and IS offerings, and to include IA and IS topics and perspectives, as appropriate, in other courses. Naturally, these efforts must be aligned with a department's foci, its current curriculum, and its accreditation requirements.

To accomplish its goals, the SEI transitions courseware, materials, and a survivability and information assurance curriculum to various departments at institutions of higher education, participates in NSF-funded faculty capacity-building programs, creates partnerships with key regional educational institutions, and offers IA symposia, among other efforts. While the SEI works with all institutions of higher education, there is a particular focus on minority-serving institutions (MSIs) and community colleges in the United States.

Rather than build a new infrastructure to accomplish this, the SEI utilizes partnerships that leverage the strengths of the SEI and the strengths of the partner educational institutions, 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 multi-pronged approach for its educational outreach in information assurance, with the goal of increasing the educational information assurance capacity.

While the focus is primarily on information security and information assurance, the SEI also includes related software engineering areas (e.g., process improvement) that are areas of core competency for the SEI and for which the SEI offers workshops for faculty and others.

1 Introduction

1.1 Prior Educational Initiatives at the SEI

From the inception of the Software Engineering Institute[1] in 1984 until 1995, the SEI's Education Program defined master's and undergraduate software engineering curricula, created materials and courses in those areas, and transitioned them to the academic and continuing education communities. Successful transition meant the educational institutions 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 the institutions' 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 CERT® Program,[2] 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 everyday life, information assurance-related topics are not limited to computer science, information science, and software engineering disciplines, but are also applicable in the areas of computer information systems, business administration, and management, to name a few examples. Information assurance education must address not only the individuals who will comprise the workforce of tomorrow, but also individuals in today's workforce, such as system and network administrators. In particular, this education should complement, not compete with, existing information security training and education. Within this context, the SEI has developed over the past three years a multi-pronged approach for its educational outreach in information assurance with the goal of increasing the nation's educational information assurance capacity.

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

[2] CERT is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

2 Current Approach

The SEI's current, multi-pronged approach for educational outreach in information assurance involves

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

The various aspects of the approach are not necessarily independent of one another, and indeed the interaction between the SEI's faculty partners and the interaction and interplay between key partner educational institutions serves to multiply the amount of educational materials available and the range of the transition activity.

Three fundamental principles are inherent in this approach:

- The SEI leverages existing efforts.
- The SEI develops complementary educational materials.
- The success of the SEI is dependent upon the success of its educational partners, whether they be faculty or the various departments in the educational institutions.

Each aspect of the approach will be discussed, in the order in which they were implemented. For the most part, later aspects build upon former aspects.

2.1 Direct Educational Outreach

Since 2002, the CERT Program has had an educational outreach program, targeting primarily historically underrepresented colleges and universities[3] (HUCUs) and Hispanic-serving institutions (HSIs), both of which fall under the larger category of minority-serving institutions. We seek departments in the areas of computer science, information science, software engi-

[3] HUCUs were previously referred to as historically black colleges and universities (HBCUs).

neering, computer engineering, and other similar departments and, in other major units of the educational institution, such as in the College of Business Administration, departments in computer information systems, or similar areas. These departments have the following characteristics:

- a desire by the department to offer, or enhance its offerings with, information security topics
- multiple faculty with an interest in this area
- a 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., a master's degree)
- strong support by the departmental chairperson
- strong support from the dean of the school
- a desire to work with the SEI to transition information security materials to the particular academic educational environment

The CERT Program offers a variety of short training courses in information security and assurance, aimed primarily at the professional workforce. These courses either enhance individuals' skills and knowledge, or enable them to learn new skills and knowledge. As stated, these are training courses, and are 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, then the SEI provided that faculty member with the courseware. Like the SEI's software engineering education model, this provided the faculty member with a "jump-start" to introduce new or additional information security topics, labs, or courses into a curriculum, as appropriate.

While this helped some faculty and some departments, it did not help those departments and faculty who met the SEI's criteria but did not yet have the necessary capabilities and capacity to take advantage of our existing materials. Leveraging the SEI's 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 CERT 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. The IACBP has initially targeted computer and information science faculty at minority-serving institutions (and later computer information systems faculty from business departments). 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 can work together with faculty from other schools that share similar interests, and who are often willing to share their own information security materials or to work collaboratively to create new materials. Finally, Carnegie Mellon's IACBP has supported multiple faculty members from the same educational institution over a period of two years to help build a critical mass at that department to better ensure the completion of its short- and long-term plans for the incorporation of information security into the curriculum. In 2004 and 2005, 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 the SEI 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 CERT materials and courseware, and to also introduce and facilitate discussions among the faculty and other CERT or SEI members who are working in areas of interest to the faculty (for example, in the areas of software process and security risk management.)

While these efforts have been successful, the CERT Program's direct educational outreach and Carnegie Mellon's IACBP program can only reach a limited number of faculty and schools each year. The challenge is how to leverage and build upon the IACBP and the CERT Program's initial educational outreach. Part of the answer lay in the creation of Regional Collaborative Clusters. This approach is helping dozens of institutions in four geographical regions improve the information assurance content in their curricula and the abilities of faculty to teach information assurance.

2.2 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; and
- are within a day's drive of one another.

At the heart of the RCC 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;

- the existence of trusted relationships with other computer science, information science, software engineering, or business (administration) departments in the immediate geographical region and beyond;
- a commitment to advance the state of information assurance education in the region through the sharing of materials and courseware, the facilitation of workshops and symposia, and other efforts;
- the 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 computer information systems departments to help create an infrastructure (the RCC) that is capable of transitioning information assurance concepts, materials, and courseware through workshops, symposia, and other means to additional educational institutions to increase the IA educational capacity in that region.

At the outset, the CERT Program and the SEI provide the hub educational transition partner with IA materials and courseware, as well as speakers for a kick-off (and a follow-on) regional IA symposium. Speakers from the SEI include not only those from the CERT Program, but also speakers in related areas, such as secure software processes and software architecture. Through the CERT, representatives from the Department of Homeland Security and the National Security Agency are also invited to speak at these regional IA symposia. Other opportunities available to the hub educational transition partner include free seats for faculty members in SEI and CERT public courses, other SEI materials and courseware (as appropriate), entrées into other Carnegie Mellon University outreach programs, and other benefits. The hub educational transition partner adapts, refines, and incorporates the IA materials and courseware as appropriate to its 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. A detailed report on these annual regional IA symposia was published in a previous report [Sledge 2005b].

The partnership between the SEI, the hub educational institution, and the Regional Collaborative Cluster is ongoing; this helps 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 rather to build upon them.

The RCC concept supports the SEI's second-level transition of information security and assurance materials and courseware 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 to share those materials with faculty, 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. Hampton's Computer Science Department Chairman, Robert A. Willis, Jr., was the key collaborator and co-developer of this 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's, existing relationships with computer science and information science departments in HUCU's within a half-day's drive of Hampton. The RCC encompasses 18 HUCU's in four states and the District of Columbia.[4] 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 [Sledge 2004].

Willis credits the first information assurance symposium held at Hampton in February 2004 with building momentum in the mid-Atlantic region: "Faculty who attended the first symposium were excited about the program and some have begun collaborations with faculty from other institutions. As the program continues, individual institutions will be better prepared to offer programs in information assurance and to start the process of certification" [Thomas 2005]. The Second Annual Hampton IA Symposium was held on April 2, 2005.

Hampton University has had four faculty attend various IACBPs and faculty from Hampton University have also taken advantage of CERT training courses and materials made available to them from those CERT training courses. Hampton University has integrated security topics into its operating systems and computer architecture courses, and into its data communication, data structure, and database management courses, with plans to continue to integrate security topics into these and other courses. Hampton is developing a new curriculum for an IA program: in 2004 and 2005, Hampton offered three courses[5], and has plans for four future courses.[6]

Two additional RCCs have been established, both targeting Hispanic-serving institutions. The first focuses on California State University campuses and community colleges in 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, with participation by California State University, Los Angeles (Cal State Los Angeles).[7] The second focuses (initially) on southern and coastal Texas with Texas A&M

---

4 See Appendix A.

5 The courses are Seminar Topics—Information Security Fundamentals, Special Topics—Information Security, and Basic Research Topics in Computer Science.

6 The courses are Network Security and Assurance, Cryptography, Information Security Implementation, and Secure Operations.

7 See Appendix B.

University, Corpus Christi (TAMU-CC) as the hub educational transition partner.[8] As at Hampton University, faculty members from Cal Poly Pomona, Mt. SAC, and TAMU-CC participated in the IACBP at Carnegie Mellon.

Dan Manson and Fred Gallegos of Cal Poly Pomona's College of Business Administration and John Blyzka and Jaishra Mehta of Mt. SAC's Computer Information Systems Department are the SEI's primary collaborators for the West Coast RCC. These hub partners can potentially help build information assurance capacity at the 23 universities in the California State University (CSU) system and at the 109 community colleges in California.

Blyzka, a computer information systems professor at Mt. SAC, reports that SEI's curriculum has been used in small business development workshops hosted by Mt. San Antonio's Small Business Development Center, and "the SEI's influence is fueling an already existing collaboration between Mt. SAC and Cal Poly Pomona with valuable information assurance resources such as source experts, curriculum, and relationships" [Thomas 2005].

Daniel Manson and Fred Gallegos, computer information systems professors at Cal Poly Pomona, have indicated the relationship with the SEI assisted Cal Poly Pomona in achieving its goal to become a National Center of Excellence in Information Assurance Education (accomplished in June 2005) [Thomas 2005].

John Fernandez and Mario Garcia of the Department of Computer and Mathematical Sciences at TAMU-CC are the SEI's primary collaborators for the Texas RCC. Garcia, an associate professor of computer science, is an exemplar of faculty who have taken advantage of multiple opportunities provided by the CERT Program: he participated in the 2003 IACBP, subsequently attended three CERT training courses[9], received the materials from those training courses, and is incorporating materials into his courses.

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 [Thomas 2005].

For example, TAMU-CC is working to build capacity at community colleges and universities in Texas, initially with those at Hispanic-serving institutions. In the future TAMU-CC also hopes to build capacity at Mexican universities with which it has relationships. As a result of the training received from CERT, 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 spent the summer of 2005 at the SEI working with members of the CERT Program in areas of mutual interest and receiving training materials

[8] See Appendix C.

[9] The courses were Information Security for Technical Staff, Advanced Information Security for Technical Staff, and Information Security for Network Managers.

for the CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). He is working to transition the knowledge and experience gained to TAMU-CC faculty and other faculty within the RCC.

Cal Poly Pomona now offers a Master in Information Assurance degree and a new program, Professional MBA in Information Assurance. Additionally, certificate programs in IA with Mt. SAC and Cal State Los Angeles are under discussion. Cal Poly Pomona and Mt. SAC held their very successful first IA Symposium on December 11, 2004. The follow-on symposium and related activities will be expanded, covering three days, December 8–10, 2005. This follow-on (and subsequent) regional symposium is planned and will be hosted by the West Coast RCC collaborators. In March 2005 Cal Poly Pomona hosted an Information Assurance curriculum development meeting. Faculty attended 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." The four schools were California State University, San Bernardino, Cal State Los Angeles, Cal Poly Pomona, and Mt. SAC, with additional faculty from other California State Universities.

Other related Cal Poly Pomona activities, which reflect the existing strength of the Cal Poly Pomona program and its newly achieved status as a National Center of Excellence in Information Assurance Education (NCEIAE), include

- the establishment of a new campus Center for Information Assurance;
- a third year of an NSF IA Curriculum project grant with Mt. SAC;
- the hosting of SEI Personal Software Process/Team Software Process Educator's Workshop (June 2005, with 22 faculty);
- the holding of a mini bootcamp (June 20–July 1, 2005) mirroring the Carnegie Mellon IACBP (and utilizing faculty from multiple educational institutions who attended the IACBP, as well as from another NCEIAE);
- the integration of information assurance throughout the Computer and Information Systems curriculum; and
- inclusion of a potential certificate program in information assurance and survivability among those under consideration by Cal Poly Pomona.

2.3 Survivability and 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. The SEI has designed and has just completed development of a three-course curriculum in survivability and information assurance (SIA).

The SIA curriculum is designed to teach system and network administrators about information assurance and to provide a way to integrate IA into their routine tasks. Administrators

need a way to think about information assurance and security issues, and they need a set of skills to help them integrate security policies, 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 1999]—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[10] 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, the principles embodied in the curriculum are the key to meeting the curriculum goals.

Because the initial target students are experienced (at least two years) system or network administrators, community colleges would logically be the first educational institutions to implement the curriculum. However, in concert with the "adapt and adopt" philosophy espoused in the CERT Program's educational outreach effort, the courses in the SIA curriculum can form the basis for a certificate program at the graduate level, or materials from the various courses can be integrated, as appropriate, into existing courses and curricula. If funding is obtained by the SEI/CERT Program, subsequent versions of the SIA curriculum produced by CERT 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, other colleges, and universities. One avenue is to work with NSF ATE centers and projects.

2.4 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 that offer information assurance training in Illinois, Minnesota, Michigan, Wisconsin, and Ohio. The center was established to address the needs of 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. It collaborates with some 75 other col-

[10] For more information, see http://www.cert.org/info_assurance/principles.html

leges and universities nationally to develop quality IT Security programs and courses. Through the SEI's relationship with CSSIA, the SEI is able to leverage CSSIA's existing relationships. The faculty at CSSIA are very knowledgeable, have an excellent plan for developing materials, transitioning those materials to the faculty, and then providing a second level of transition to other faculty in the regional area.

The SEI has licensed three CERT courses[11] to CSSIA, which will adapt materials from these courses into their courses. In March 2005, Sledge presented an overview of the SIA curriculum to the CSSIA Board of Visitors. With the completion of the development of the SIA curriculum, the SEI will transition those courses to CSSIA for adaptation and dissemination to interested CSSIA partners for academic use. Spengler has stated, "The partnership greatly increases the community and technical college system's ability to respond to the challenges of adapting, disseminating, and delivering quality, industry-recognized information assurance and cyber security curriculum to students and faculty" [Thomas 2005].

2.5 Leveraging State University Systems

Through the SEI's relationships with faculty at Cal State Los Angeles and Cal Poly Pomona, we were able to present our CERT educational outreach programs and our Survivability and Information Assurance Curriculum to the Computer Science/Information Science/Software Engineering/Computer Information Systems/Management Information Systems discipline council, which comprises department heads in those disciplines from the 23 California State University campuses. This discipline council meets to discuss relevant issues from a California State University-wide perspective. Working with a number of the departments represented on the council, we are seeking to directly transition our IA materials and courseware. However, we believe the most effective transition to and through the discipline council will come from its members working together to include appropriate information security and information assurance content in, for example, certain general education courses, to provide training opportunities for their fellow faculty members in information assurance, to work to incorporate and share information security courses, and to work closely together in the area of information security with community colleges in California (through potential articulation programs). While this effort is in just the beginning "thought" stages by various faculty and chairs in the CSU system and certain community colleges, we look forward to short, mid- and long-term results of a successful effort and will endeavor to support it.

Six California State University System campuses (all HSIs) participated in the 2005 IACBP at Carnegie Mellon University. This included returning institutions (California State Polytechnic University, Pomona; California State University, Los Angeles) and new institutions (California State University, Northridge; California State University, Fresno; California State University, Dominguez Hills; San Jose State University). Faculty represented departments within colleges of business administration and engineering, and departments of computer sci-

[11] The courses are Information Security for Technical Staff, Advanced Information Security for Technical Staff, and Information Security for Network Managers.

ence and software engineering. Based on the strengths of these institutions and the dedication of their faculty, we believe a critical mass has been achieved to support the continued transition and incorporation of information security and information assurance materials within the California State University system. By continuing to work individually with campuses in the CSU system and working with the discipline council, we hope to learn lessons that can be applied to other state university systems.

3 Other Leverage Points

3.1 Cross Departmental/Cross College

Another aspect of transition and leverage is the cross departmental/cross college work established at Cal State Los Angeles: Parviz Partow and Ludwig Slusky, from the Department of Information Systems, College of Business and Economics, work with Le Tang of the Department of Technology, College of Engineering, Computer Science, and Technology. All three professors attended the IACBP (the first two in 2004 and Tang in 2005).

The Department of Information Systems is making modifications to incorporate information assurance and security topics in three undergraduate and two graduate level courses and has introduced or plans to introduce two new undergraduate courses. The department is also working on a general education course, an introduction to information security, and on the addition of an information security track to a campus-wide information technology minor. Tang is working on an information security certificate program, which will require approvals from two departments in two different colleges at Cal State Los Angeles.

Weider Yu of San Jose State University plans to engage in information assurance curriculum activities with faculty in his Computer Engineering Department and, through his contacts, to support information assurance curriculum development in the Computer Science Department in the College of Science and in the Management Information Systems Department in the College of Business. In addition to the materials from the 2005 IACBP, Yu has also received (for academic use) three CERT courses.[12]

3.2 Associations

The CERT Program 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

[12] The courses are Information Security for Technical Staff, Advanced Information Security for Technical Staff, and Information Security for Network Managers.

information assurance and the incorporation of information assurance topics and courses in their curricula.

The Association of Computer/Information Sciences and Engineering Departments at Minority Institutions (ADMI) "was established as a national organization dedicated to exploring and providing remedies to the educational issues in computer/information science and computer engineering that confront minority institutions of higher education."[13] ADMI holds an annual symposium, and since 2004, CERT and the SEI have participated in these symposia [Sledge 2004].

3.3 Within Carnegie Mellon University

The SEI is one of eight units within Carnegie Mellon University and the SEI seeks to transition information assurance content within the university. The Information Systems program in the College of Humanities and Social Sciences (H&SS) has a junior level, team-based software development project course. In Spring 2005, five of the lectures were devoted to information security/assurance topics and were taught by representatives of the CERT program, with the intent of transitioning this material and the ability to teach it to the H&SS faculty. A member of the CERT Program participated in an H&SS summer program, "Information Systems in the Community," which targets computer science/information science majors from HUCUs entering their senior year.

Ancillary activities, not directly influenced by the work described here, are the teaching, by members of the CERT Program, of various information security/information assurance courses in the H. John Heinz III School of Public Policy and Management, and in the Information Networking Institute (within the Carnegie Institute of Technology, Carnegie Mellon's engineering college).

3.4 Between Major Educational Partners

Finally, although in some cases our relationships with our educational partners are less than 24 months old, we can look forward in the not-too-distant future to the ultimate leverage: those educational partners working together and sharing derivative and enhanced materials they have adapted from our materials, in addition to the materials they have developed. We believe Dan Manson of Cal Poly Pomona and Erich Spengler of CSSIA will be among the first to find mutually beneficial sharing opportunities.

[13] See http://cerser.ecsu.edu/admi2005/.

4 Future Work

4.1 Future RCCs

Oakwood College, an HUCU, has participated in the 2004 and 2005 IACBP. Oakwood faculty have also attended CERT training courses and are incorporating additional information security content and courses into their curriculum, and are working with other departments within their college. Oakwood is in the preliminary planning stages to establish itself as an RCC, targeting HUCUs in Alabama, Tennessee and Mississippi.[14]

4.2 New CERT Technology

CERT has recently completed the initial development of a Virtual Training Environment (VTE), which provides Web-based, individual training on information assurance and information technology topics. VTE leverages the various CERT curricula materials. It utilizes a knowledge library model: it is self-paced and searchable, with quick access to specific topics. In fall 2005, one institution will pilot the use of VTE as a resource for curriculum development at graduate schools.

[14] See Appendix D.

5 Summary

This report is an expansion of an earlier paper on educational outreach initiatives at the SEI [Sledge 2005a].

Through its CERT 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 everyday 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 must 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 multi-pronged approach for its educational outreach in information assurance with the goal of increasing IA educational capacity.

This multi-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 (comprising colleges, universities and community colleges);
- creating a survivability and information assurance curriculum;
- working with National Science Foundation Advanced Technological Education projects and centers to reach community colleges, colleges and universities; and
- leveraging state university systems.

Since 2002, the CERT Program has had an educational outreach program, targeting selected minority-serving institutions and working individually with those institutions. While a 1:1 approach can transition materials, it is not the most efficient method. 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, which serves as our key collaborator in creating, building, and sustaining an IA Regional Collaborative Cluster. By leveraging that partner's strengths and the SEI's strengths, we can 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

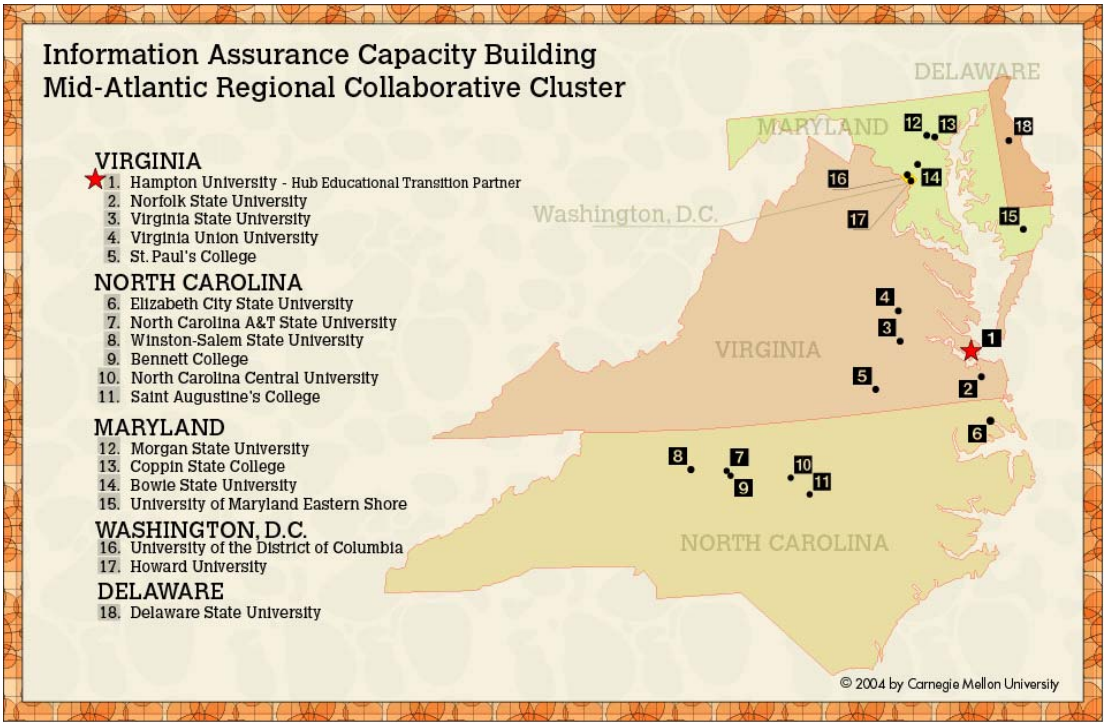
and adapt materials to their particular curricula, and share those materials with other faculty and colleges and universities.

To address the needs of system and network administrators, CERT recently finished development of a three-course curriculum in survivability and information assurance. These courses can be offered through community colleges, and can be adapted for use in undergraduate and graduate 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.

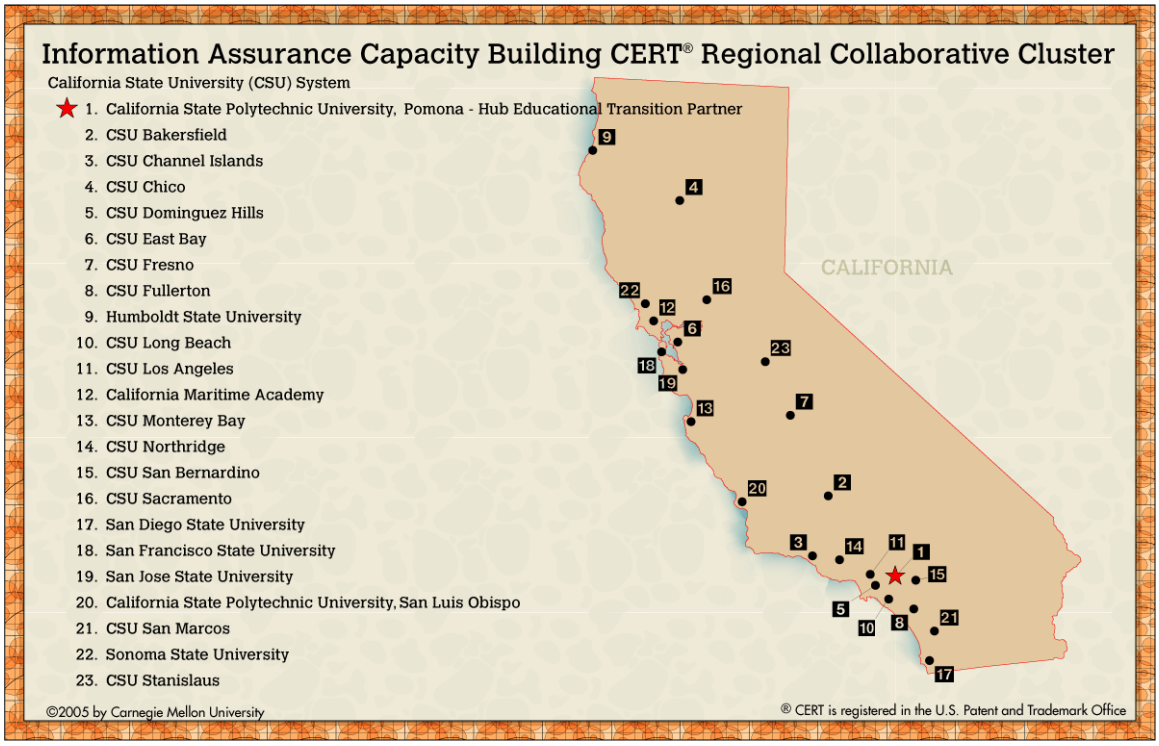
One of our goals is for our various educational partners to adapt, adopt, and expand what we provide to those educational institutions within their various regions. Ultimately, we hope these hub educational partners will work with one another to leverage what they individually have developed. Another potential avenue for this is state university systems: initial work with various campuses within the California State University system shows some promise for that work to be expanded throughout the system.

We seek to complement, not compete with, other programs. Leveraging other complementary programs, events, and organizations broadens the educational offerings and makes it more cost effective to all parties concerned. As always, we judge our success by the success of our education transition partners.

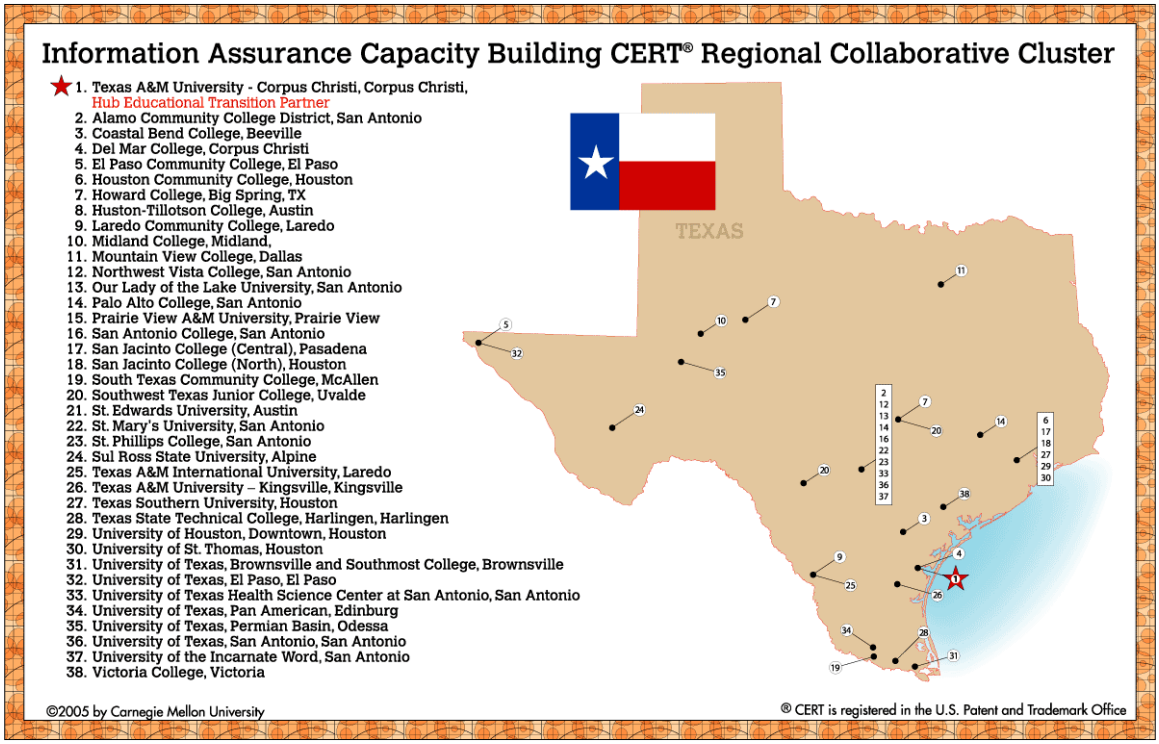
Appendix A Mid-Atlantic Regional Collaborative Cluster



Appendix B West Coast Regional Collaborative Cluster



Appendix C: Texas Regional Collaborative Cluster



Appendix D Proposed Southern Regional Collaborative Cluster; Targeted HUCU Institutions (AL, TN, MS)

Oakwood College: Hub Educational Transition Partner
Alabama A&M University
Alabama State University
Alcorn State University
Bishop State Community College
Coahoma Community College
Concordia College
Fisk University
Hinds Community College
J.F. Drake State Technical College
Jackson State University
Knoxville College
Lane College
Lawson State Community College
Lemoyne-Owen College
Mary Holmes College
Meharry Medical College
Miles College
Mississippi Valley State University
Rust College
Selma University
Shelton State Community College
Stillman College
Talladega College
Tennessee State University
Tougaloo College
Trenholm State Technical College
Tuskegee University

References

URLs are valid as of the publication date of this document.

[Lipson 1999] Lipson, Howard & Fisher, David. "Survivability—A New Technical and Business Perspective on Security." *Proceedings of the 1999 New Security Paradigms Workshop*. Association for Computing Machinery. New York, 1999. Also available at http://www.cert.org/archive/pdf/busperspec.pdf.

[Sledge 2004] Sledge, Carol A. & Willis Jr., Robert. "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*. Orlando, FL, May 2004. ADMI: May 2004.

[Sledge 2005a] Sledge, Carol A. "Information Assurance Educational Outreach: Initiatives at the Software Engineering Institute." *Proceedings from the Ninth Annual Colloquium for Information Systems Security Education (CISSE)*, 6-9 June 2005, Georgia Institute of Technology, Atlanta, GA. ISBN: 1-933510-99-4.

[Sledge 2005b] Sledge, Carol A. *Report on Annual Regional Information Assurance Symposia*, CMU/SEI-2005-SR-007. Pittsburgh, PA, June 2005. Also available at http://www.sei.cmu.edu/publications/documents /05.reports/05sr007.html

[Thomas 2005] Thomas, Bill. "University Hubs Help SEI Spread Information Assurance Curricula and Methods." *news@sei 8*, 1 (2005): 8-9. Also available at http://www.sei.cmu.edu/publications/news-at-sei /features/2005/1/feature-3-2005-1.htm

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	September 2005	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Building Information Assurance Educational Capacity: Pilot Efforts to Date	FA8721-05-C-0003

6. AUTHOR(S)

Carol A. Sledge, Ph.D.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2005-SR-009

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report describes efforts by the Software Engineering Institute (SEI) to increase the capacity of institutions of higher education to offer information assurance (IA) and information security (IS) courses, to expand existing IA and IS offerings, and to include IA and IS topics and perspectives, as appropriate, in other courses.

To accomplish these goals, the SEI transitions courseware, materials, and a survivability and information assurance curriculum to various departments at institutions of higher education, participates in NSF-funded faculty capacity-building programs, creates partnerships with key regional educational institutions, and offers IA symposia, among other efforts. While the SEI works with all institutions of higher education, there is a particular focus on minority-serving institutions.

Rather than build a new infrastructure to accomplish this, the SEI utilizes partnerships that 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.

14. SUBJECT TERMS	15. NUMBER OF PAGES
information assurance education, information security education, regional collaborative cluster, capacity building	37

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL