CERIAS Tech Report 2004-107
Adaptation of a State of the Art Computer Forensics Course

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

Information Assurance: Building Educational Capacity

Carol A. Sledge, PhD

June 2006

SPECIAL REPORT
CMU/SEI-2006-SR-007

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Information Assurance: Building Educational Capacity

CMU/SEI-2006-SR-007

Carol A. Sledge, PhD

June 2006

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.

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

This report is the fourth in a series describing the efforts by the Software Engineering Institute (SEI), and in particular those of its CERT® Program to increase the capacity of institutions of higher education to offer information assurance (IA) and information security (IS) courses. Other goals are to expand existing IA and IS offerings and to include IA and IS topics and perspectives in other courses. For each participating institution, these efforts are aligned with the focus of its involved academic department, current curriculum, and accreditation requirements. The report describes SEI activities for accomplishing its goals: participating in faculty capacity building programs funded by the National Science Foundation; creating and transitioning courseware, materials, and a newly created survivability and information assurance curriculum; and collaborating with key regional educational institutions. This report also presents four approaches the SEI has developed for its educational outreach in IA. The SEI applies these approaches as it works with all institutions of higher education, with a particular focus on minority-serving institutions and community colleges in the United States.

1 Introduction

1.1 Background

The past decade has seen commercial organizations, governmental and nongovernmental organizations, academic institutions, and individuals embrace a network-centric (or net-centric) view of their respective and aggregate worlds. With the economies, efficiencies, and opportunities of this net-centric world have come new challenges, threats and shifts in paradigm, perspective, operation, and strategy—all on an increasingly compressed time scale. The magnitude and frequency of these changes demand a workforce that is

- skilled in information assurance and survivability
- empowered to mitigate and eliminate errors in operational practices and management that leave organizations vulnerable to a variety of attacks, failures, and accidents
- capable of mitigating and eliminating errors in the design, development, and implementation of the technologies that support today's net-centric worlds

The network-centric world also strongly affects individuals outside of the work environment. They find that their computers, mobile devices, and Internet-based social and financial transactions mirror the challenges and needs of the workplace.

The Software Engineering Institute,[1] through its CERT® Program,[2] works with U.S. Department of Defense (DoD) customers and the U.S. government. Through this work the SEI develops, delivers, and transitions curricula, instruction, and certification in information assurance and computer network defense. These curricula are designed for system and network administrators, managers, executives, and educators. The SEI also develops and releases materials covering many topics, including the adoption and use of security and survivability practice.

In its initial decade, the Software Engineering Institute (SEI) engaged in the transition of software engineering curricula and course materials. Through CERT, the SEI is again engaged in transitioning curricula, 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

[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.

everyday life, information assurance-related topics are not limited to computer science, information science, or software engineering disciplines. These topics also apply to 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 compose 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, CERT has developed, over the past four years, a multi-pronged approach for its educational outreach in information assurance with the goal of increasing the nation's educational information assurance capacity.

2 Approach

The SEI/CERT approach for educational outreach in information assurance 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)
- working with the Center for Systems Security and Information Assurance, a National Science Foundation (NSF) Advanced Technological Education (ATE) regional center, to reach, primarily, community colleges, colleges, and universities
- leveraging state university systems
- participating in an NSF-funded Information Assurance Capacity Building Program (IACBP)
- creating and transitioning a survivability and information assurance curriculum

These aspects of the approach are often interdependent, and the interaction between the SEI's faculty collaborators and the interaction and interplay between key educational institutions serves to multiply the amount of educational materials available and the range of the transition activity.

Inherent in this approach are three fundamental principles:

- The SEI develops educational materials that complement those already available.
- The SEI leverages existing efforts.
- The success of the SEI is dependent upon the success of its educational collaborators, whether they be faculty or various departments of the educational institutions.

Each aspect of the approach will be discussed in the following sections. Many of the aspects build upon or leverage other aspects of the approach, with faculty and educational institutions participating in multiple aspects of the approach.

2.1 Institutions of Higher Education

Since 2001, the CERT Program has carried on an educational outreach program to institutions of higher education. These include community colleges, colleges, and universities, undergraduate and graduate programs. Carnegie Mellon University[3] is committed to interdisciplinary research and education, not only within and across academic fields, departments, schools, and colleges, but also across institutional, national, and cultural boundaries. Carnegie Mellon embraces diversity as a core value—central to and inseparable from the pursuit of intellectual and artistic excellence. Because of Carnegie Mellon's commitment to diversity, CERT has especially reached out to historically underrepresented colleges and universities[4] (HUCUs) and Hispanic-serving institutions (HSIs), both of which fall under the larger category of minority-serving institutions (MSIs).

The SEI/CERT seeks departments in the areas of computer science, information science, software engineering, computer engineering, and other similar areas. Departments are also sought 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 members with an interest in this area
- a long-range goal of offering information security/information assurance courses leading to a professional degree (e.g., a master's degree) or to a concentration/certificate program/option at the undergraduate or graduate level
- 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 SEI works directly with these departments, but also seeks to leverage its strengths, as well as the strengths, contacts, and relationships of the department and its faculty, to increase the educational capacity to teach information security and information assurance. One way to do this is through the creation of Regional Collaborative Clusters. This approach targets dozens of institutions in four geographical regions to 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 with each other in the past, or can reasonably be expected to cooperate

[3] The Software Engineering Institute is one of the eight major units of Carnegie Mellon University.

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

- have a desire to incorporate or expand their information assurance content
- 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
- 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
- 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. This enables the creation of 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. The goal is to increase the information assurance (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 kick-off and follow-on regional IA symposiums. 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 CERT, representatives from the Department of Homeland Security have also been 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, additional 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)
- hosts other IA-related workshops

The hub educational transition partner completely takes over responsibility for the regional IA symposium no later than its third year as a partner.

The initial, prototype RCC, the Mid-Atlantic Regional Collaborative Cluster, was established in 2003, with Hampton University as the hub educational partner. 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 existing relationships, and, in particular, Willis's relationship, with computer science and information science departments in HUCUs within a half-day drive of Hampton. The RCC encompasses 18 HUCUs in four states and the District of Columbia [see Appendix A]. 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 were presented in a paper by Sledge and Willis at the 2004 ADMI Symposium.[5]

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 05].

The Second Annual Hampton IA Symposium was held on April 2, 2005.

Two additional RCCs have been established, both targeting Hispanic-serving institutions. The first focuses on California State University campuses and community colleges in California. California State Polytechnic University, Pomona (Cal Poly Pomona) and neighboring Mt. San Antonio Community College (Mt. SAC) of Walnut, CA, are the hub educational transition partners. California State University, Los Angeles (Cal State Los Angeles), also participates [see Appendix B]. The second RCC has initially focused on southern and coastal Texas with Texas A&M University, Corpus Christi (TAMU-CC), as the hub educational transition partner [see Appendix C].

Oakwood College, an HUCU, is in the preliminary planning stages to establish itself as an RCC, targeting HUCUs in Alabama, Tennessee, and Mississippi [see Appendix D].

[5] 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.

Although the three established RCCs share similarities, the RCCs and their hub educational transition partners also exhibit dissimilarities. These differences reflect not only the SEI 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 05]. Information on the activities of the hub educational institutions of the three established RCCs is contained in Appendix E and in a previous report [Sledge 05c].

A detailed report on the annual regional IA symposia associated with the three established RCCs was published previously [Sledge 05b]. Since that report, Cal Poly Pomona took over total control of its IA Symposia and produced a symposium to reflect its interests and strengths. A well-attended and very successful Second Annual Information Assurance Symposium (IAS) was held December 8-10, 2005, at the Kellogg West Conference Center. The IAS solicited papers (including student papers), tutorials, and workshop proposals for both a curriculum track and a compliance track. The IAS also included invited keynote speakers and held a day of panel discussions.

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 or other grant-funded local and regional work that the partner institution may have). 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 second-level transition of information security and assurance materials and courseware to surrounding educational institutions through the hub educational transition partner. The SEI’s 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.

Another approach to leveraging educational outreach to help increase the capacity to teach information assurance is to work with National Science Foundation (NSF) Advanced Technological Education (ATE) regional centers, specifically the Center for Systems Security and Information Assurance (CSSIA).

2.3 Center for Systems Security and Information Assurance

The Center for Systems Security and Information Assurance [CSSIA 06], an NSF Regional Center based at Moraine Valley Community College in Palos Hills, IL, is the first comprehensive IT security center in the Midwest, according to its director Erich Spengler. The center itself includes seven 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 more than 100 other colleges and universities nationally to develop quality IT Security programs and courses.[6] Through the SEI's relationship with CSSIA, the SEI is able to leverage CSSIA's existing relationships. The faculty at CSSIA are very knowledgeable and have an excellent plan for developing materials, transitioning those materials to faculty, and then providing a second level of transition to other faculty at community colleges and colleges in the regional area. If space is available, faculty from community colleges, colleges, and universities outside the region can also attend CSSIA offerings.

There are two current ways in which the SEI is leveraging its collaborative relationship with CSSIA. 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' existing skills and knowledge or introduce them to new knowledge and skills. As stated, these are training courses and are not necessarily in the form or format of an academic offering in an institution of higher education. However, courseware was provided by the SEI to a faculty member who already had the capacity to understand these training materials, could adapt and adopt this courseware for use in his or her courses and curriculum (academic-use only), and who was willing to share the derivative educational materials.[7] This provided the faculty member with a "jumpstart" 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 its existing materials. It also could reach only a small number of faculty. The SEI has licensed three CERT courses[8] to CSSIA, which can adapt materials from these courses into its courses or offer CERT courses in their original form to faculty for their academic credit use.

With the completion of its Survivability and Information Assurance Curriculum, the SEI has also transitioned 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 05].

[6] For more information, see http://www.cssia.org/partner_directory.cfm.

[7] This applies to a subset of the current CERT training courses.

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

2.4 Leveraging State University Systems

Through the SEI's relationships with faculty at California State University, Los Angeles, and California State Polytechnic University, Pomona, the SEI was able to present its CERT educational outreach programs and its Survivability and Information Assurance Curriculum. It was also able to promote the Information Assurance Capacity Building Program 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 (CSU) 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, the SEI is seeking to directly transition its IA materials and courseware. However, the most effective transition to and through the discipline council is expected to result from council members' working together. Their work might serve, for example, to include appropriate information security and information assurance content in certain general education courses or to provide training opportunities for fellow faculty members in information assurance. The council might also cooperate to incorporate and share information security courses and 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, the SEI looks forward to short-, mid-, and long-term results of a successful effort.

The SEI involvement with an NSF-funded Information Assurance Capacity Building Program (IACBP) held at Carnegie Mellon University provides the opportunity to leverage and expand its involvement with the California State University system and to enlarge the set of faculty with the capacity to teach information security and information assurance topics. Of the 11 California State University System campuses designated as HSIs, 6 have participated in this capacity building program, and a seventh California State University HSI campus will participate in 2006. But participation in the IACBP is broader than this.

2.5 Information Assurance Capacity Building Program

Since 2002, members of the CERT Program at the SEI have helped select faculty and since 2001 have designed and participated yearly in a month-long, NSF-funded Information Assurance Capacity Building Program at Carnegie Mellon University. Carnegie Mellon has certification as both an NSF Cyber Trust Center and National Security Agency-designated Center of Academic Excellence (CAE) in Information Assurance Education.

The IACBP 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, including current research topics, provides additional course material, and offers networking and mentoring opportunities with other faculty and researchers. This provides faculty with the opportunity to create short- and long-term plans for the incorporation or expansion of information security/assurance topics and courses into their curriculum, as appropriate. Moreover, the faculty at one capacity building program can work together with faculty from other schools that share similar interests, and are often willing to share their own information security materials or to work collaboratively to create new materials. Finally, for several institutions, Carnegie Mellon's IACBP has leveraged another strategy. For each institution, the IACBP has supported multiple faculty members from that institution over a period of two years. This has helped build a critical mass at that institution's department to better ensure the completion of its short- and long-term plans for the incorporation of information security into the curriculum. Beginning in 2004 the IACBP added faculty from business departments that have strong information systems components and thus an interest in enhancing the information assurance coverage in their curricula.

The first four offerings of the Information Assurance Capacity Building Program have exceeded the expectations of its participants and have made a measurable impact on the capacity of the engaged minority-serving institutions to educate students in information assurance. In other words, they have been deemed a resounding success. The SEI has forged strong ties with a number of minority-serving institutions. Through these and related SEI/CERT approaches the SEI has significantly increased the ability of these institutions to address information assurance in their Computer Science, Computer Information Systems, and Business curricula. The program has resulted in the development of a number of new offerings at SEI partner schools, from short modules integrated into pre-existing courses to full courses, IA certificates, and even plans and initial frameworks for master's degree programs in IA. The program has also led to a number of research projects and publications involving faculty and students at partner schools, as well as multi-institution regional collaborative clusters. In 2004 and 2005, participants have included 17 faculty (including two department chairs) in computer and information science, computer information systems, and similar departments from 11 minority-serving institutions. See Appendix E for a sample of the impact and results achieved by the participating faculty.

Participants in the capacity-building program go on to create an immediate impact at their home institutions, both on an individual and department-wide scale. For example, Dr. David Miller of the Department of Accounting and Information Systems, California State University, Northridge, attended the 2005 capacity building program. Dr. Miller came to the program with the intention of creating an IA course called "Special Topics in Information Systems, Information Security and Assurance," an upper-division elective for students majoring in information systems. Miller developed the content for the course during the program in the summer and was then able to offer it in the fall semester. The course was immediately in high demand—all forty-one available seats were filled, spilling over onto a waiting list. The course has since become an approved regular offering in the university's curriculum, and it is the foundation for a full information assurance curriculum that the department hopes to create.

As we have seen, faculty who attend the IACBP return to their home institutions with the ability to substantially enhance the information assurance capacity of their schools. Additionally, through the relationships they develop among themselves during the month-long program, they also work together to provide opportunities for other faculty in their geographic regions, including the emulation of the IACBP.[9] Because of the 2005 capacity building program, collaboration between several members of the California State University (CSU) system has begun. Five CSU schools have begun to work together to create modules, topics, and courses that can be developed and distributed among the CSU system's 23 campuses. This also leverages the SEI's prior and ongoing work with the CSU discipline council in the departments within colleges of business administration and engineering, and departments of computer science and software engineering. Finally, in the CSU system, students are encouraged to attend community colleges before entering the universities, and the SEI recruited and incorporated Mount San Antonio College into the capacity building program to further spread the impact and enhancement of IA educational capacity into California's 109-campus community college system. Based on the strengths of these institutions and the dedication of their faculty, it appears that a critical mass has been achieved to support the continued transition and incorporation of information security and information assurance materials within the CSU system. By continuing to work individually with campuses in the CSU system and working with their CSU discipline council, the SEI hopes to learn lessons that can be applied as it expands its approach to other state university systems.

A side benefit of the month-long capacity building 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. Through these meetings the SEI can 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). It is worth noting that discussions that led to the formation (or proposal to form) RCCs had their start during after-hours meetings in the month-long IACBPs.

One example of transition of relevant CERT materials and courseware to faculty during the offering of the IACBP is the SEI Survivability and Information Assurance curriculum.

[9] Manson, D.; Corey, S.; Fernandez, J. Blyzka, J.; Farkas, R.; Partrow, P.; & Garcis, M. "Beyond Bootcamps: A model for ongoing curriculum development collaboration for faculty attending and Information Assurance bootcamp." This paper was presented to the Secure IT 2005 Conference, San Diego, CA, April 19-22, 2005.

3 Survivability and Information Assurance Curriculum

The SEI has designed, developed, and released a three-course, 13-semester-hour (162.5 total hours) curriculum in survivability and information assurance (SIA). The Survivability and Information Assurance 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 infrastructures. The goal is to produce a more secure and predictable operational state.

In addition, survivability—which CERT defines 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—is a relatively new responsibility for the entire organization, including system and network administrators [Lipson 99]. System and network administrators need to know their roles and how to achieve the goals of survivability.

The SIA curriculum is based upon 10 principles that are emphasized throughout each course [CERT 06]. 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 have at least two years experience in system or network administration, community colleges would logically be the first educational institutions to implement the materials in 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. Ideas and topics can be used without commitment to an entire course or the entire curriculum and can be adapted and/or expanded to fit the focus of a department’s wider curriculum and the constraints of accreditation. The SIA curriculum is designed to be adapted and adopted by institutions of higher education to suit their needs.

3.1 Topic Areas

The SIA curriculum consists of three major topic areas, each of which is a course within the curriculum:

- Principles of Survivability and Information Assurance
- Information Assurance Networking Fundamentals
- Sustaining, Improving, and Building Survivable Functional Units

Principles of Survivability and Information Assurance consists of a three-semester-credit-hour course and a separate one-semester-credit-hour lab. The lab component introduces the basics of the technology required for the next course. Therefore, the lecture portion of this first course can be offered to managers of system and network administrators, who may not have sufficient background for the remaining courses.

Information Assurance Networking Fundamentals is structured as a five-semester-credit-hour course, with the labs closely integrated with the lectures. The addition of the optional labs makes this a six-semester-credit-hour course, or two three-semester-credit-hour courses. This course applies the 10 principles of survivability and information assurance to the concepts and implementation of TCP/IP networking. In particular, understanding and challenging the assumptions made by the TCP/IP protocols and then considering the risks to the enterprise when using these protocols is a critical part of the discussions.

Sustaining, Improving, and Building Survivable Functional Units,[10] the capstone course, is a four-semester-credit-hour course, with the lab component closely integrated with the lectures. Unlike in the first two courses, students work mostly in teams for the capstone course. They inherit an existing enterprise network, utilize information from the second course to understand the underlying structure of the inherited network, manage it according to the 10 principles, improve the survivability of the existing functional units in that network, and add a new survivable functional unit to the improved network.

3.2 Materials and Availability

The Survivability and Information Assurance curriculum materials were developed for use by qualified faculty from appropriate departments at institutions of higher education. All files associated with the courseware and supplemental lab materials, including detailed faculty and student workbooks, quizzes, exams, exercises, and suggested answers, are freely available to qualified faculty who accept the SIA licensing agreement and complete the required faculty request form. The information on this form must be validated by institute personnel to ensure that SEI criteria are met before access to the faculty download site is granted. Curriculum-

[10] Survivable Functional Units are explained in “Balancing an Enterprise’s Mission and Technology” (http://www.cert.org/archive/pdf/04tn004.pdf).

wide information and access to the SIA license, required (faculty request) forms, and the faculty download site is available at http://www.cert.org/sia/.

A subset of the SIA curriculum materials, Adobe Acrobat PDF files of the curriculum-wide information and student (not faculty) materials, is freely available on that same http://www.cert.org/sia/ site to any interested person who accepts the SIA licensing agreement and completes the required general access form. Unlike with the faculty download site, once the SIA licensing agreement is accepted and the required general access form completed, there is immediate access to this general access subset of the SIA curriculum materials. In terms of hard copy pages of materials, the general download site consists of approximately 2800 pages, while the faculty download site consists of approximately 6000 pages.

The SIA curriculum site, http://www.cert.org/sia/, became available during the last week of January 2006. As of June 28, 2006, 769 downloads from 80 countries had occurred on the general area with the following breakdown of affiliation: 256 company, 196 personal, 152 educational, 125 governmental agency and 40 “other.” As of that same date, 90 validated faculty from 75 educational institutions had received access privileges to the SIA curriculum faculty download area.

As with its 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, four-year colleges, and universities. As mentioned earlier, the SEI has transitioned this curriculum to CSSIA for adaptation and dissemination to interested CSSIA partners for academic use. CSSIA has also placed a link on its Web site to the CERT SIA curriculum site. In addition, faculty attending the month-long IACBP are given the faculty version of the SIA curriculum and encouraged to promote its availability to other faculty who may have an interest in the materials.

4 Summary

This report is the fourth in a series on educational outreach initiatives at the SEI [Sledge 05a, Sledge 05b, Sledge 05c].

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 compose 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. Within this context, the SEI has developed, over the past four years, 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 (colleges, universities, and community colleges)
- working with the Center for Systems Security and Information Assurance (CSSIA), a National Science Foundation Advanced Technological Education regional center to reach (primarily) community colleges, colleges, and universities
- leveraging state university systems
- participating in an NSF-funded Information Assurance Capacity Building Program
- creating and transitioning a survivability and information assurance curriculum

Many of the aspects build upon or leverage other aspects of the approach, with faculty and educational institutions participating in multiple aspects of the approach.

Since 2001, the CERT Program has had an educational outreach program, with a particular emphasis on selected minority-serving institutions and working individually with those institutions. While this one-on-one approach can transition materials and build capacity, it is not the most efficient method. By building upon existing trusted relationships and infrastructure, the SEI can effectively extend its reach. One way to do this is to work with a hub educational transition partner, which serves as the SEI’s key collaborator in creating, building, and sustaining an IA Regional Collaborative Cluster. By leveraging that partner’s strengths and the SEI’s strengths, the partnership can work to increase the number of information security topics and courses in the curricula of the participating schools in the RCC. The SEI/CERT 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.

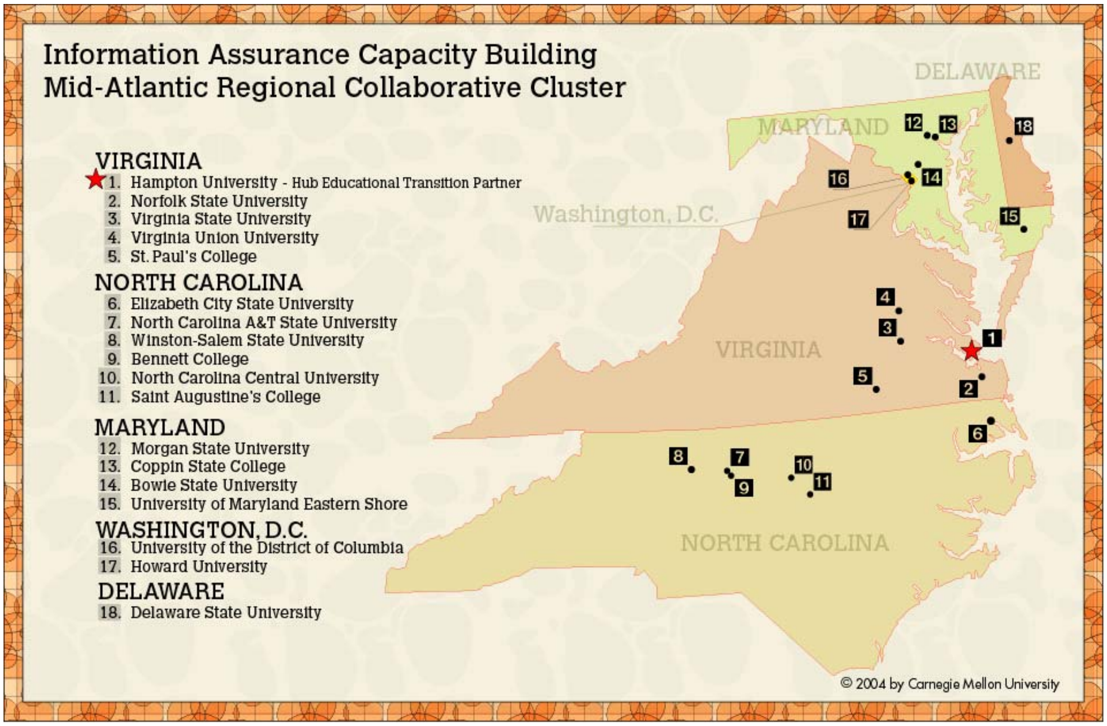
Another way to extend reach is to work with state university systems. CERT’s educational outreach includes working directly with faculty from a number of the campuses in the California State University System, as well as addressing the 23-campus departmental discipline council meetings.

Through its involvement with the Information Assurance Capacity Building Program at Carnegie Mellon and related efforts with other aspects of its approach, the SEI/CERT has achieved broad impact since 2001. The response from faculty members who have participated in this capacity building program, as well as from their department heads, has been uniformly and extremely positive. The development of a number of new offerings at participating schools, from short modules integrated into pre-existing courses to full courses, IA certificates, and even plans and initial frameworks for master's degree programs in IA, has resulted. This capacity building program has also led to a number of research projects and publications involving faculty and students at participating schools, as well as the multi-institution regional collaborative clusters. All further enhance the nation’s educational capacity in information assurance.

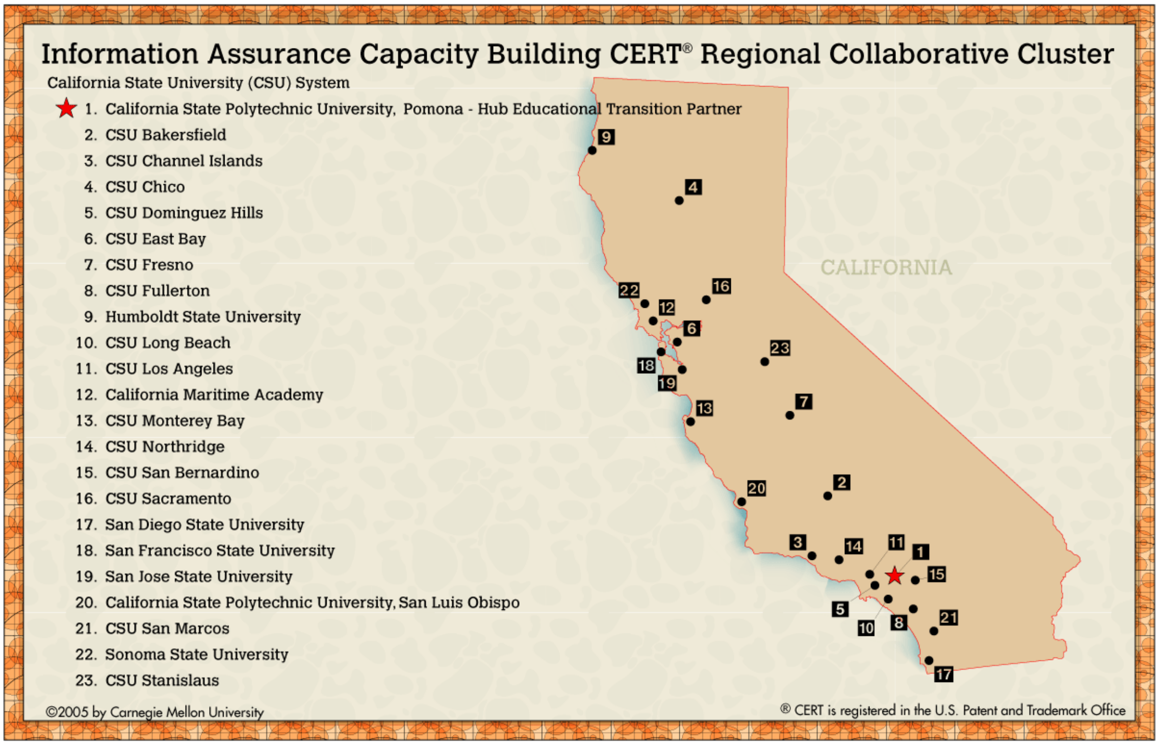
To address the needs of system and network administrators, CERT recently finished development of a three-course curriculum in survivability and information assurance. These courses can be offered through community colleges and universities and can be adapted for use in both undergraduate and graduate programs. One avenue for transition to community colleges is the working through and leveraging of the work being done by Center for Systems Security and Information Assurance, an NSF ATE center, one of the SEI’s key educational collaborators.

The SEI/CERT seeks 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, the SEI/CERT judges its success by the success of its education transition partners and collaborators.

Appendix A: Mid-Atlantic Regional Collaborative Cluster


Information Assurance Capacity Building
Mid-Atlantic Regional Collaborative Cluster
VIRGINIA
★ 1. Hampton University - Hub Educational Transition Partner
2. Norfolk State University
3. Virginia State University
4. Virginia Union University
5. St. Paul's College
NORTH CAROLINA
6. Elizabeth City State University
7. North Carolina A&T State University
8. Winston-Salem State University
9. Bennett College
10. North Carolina Central University
11. Saint Augustine's College
MARYLAND
12. Morgan State University
13. Coppin State College
14. Bowie State University
15. University of Maryland Eastern Shore
WASHINGTON, D.C.
16. University of the District of Columbia
17. Howard University
DELAWARE
18. Delaware State University
DELAWARE
MARYLAND
Washington, D.C.
VIRGINIA
NORTH CAROLINA
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
© 2004 by Carnegie Mellon University

Appendix B: West Coast Regional Collaborative Cluster



Information Assurance Capacity Building CERT® Regional Collaborative Cluster

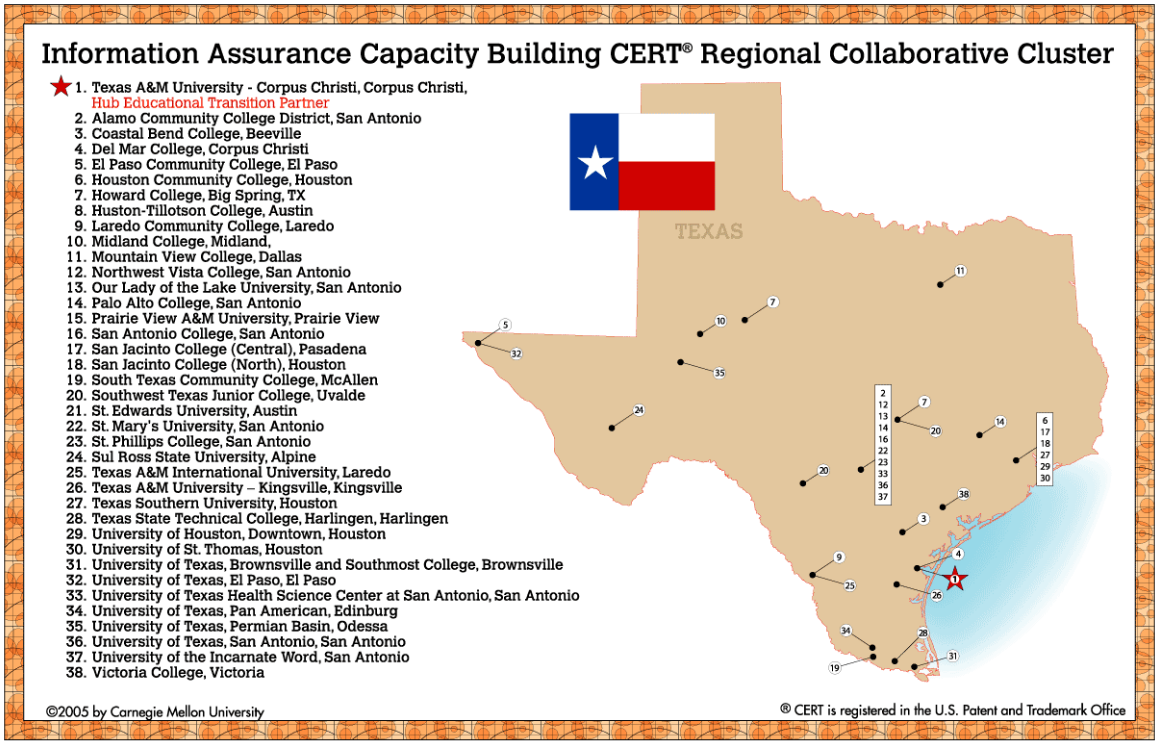
California State University (CSU) System

★ 1. California State Polytechnic University, Pomona - Hub Educational Transition Partner
2. CSU Bakersfield
3. CSU Channel Islands
4. CSU Chico
5. CSU Dominguez Hills
6. CSU East Bay
7. CSU Fresno
8. CSU Fullerton
9. Humboldt State University
10. CSU Long Beach
11. CSU Los Angeles
12. California Maritime Academy
13. CSU Monterey Bay
14. CSU Northridge
15. CSU San Bernardino
16. CSU Sacramento
17. San Diego State University
18. San Francisco State University
19. San Jose State University
20. California State Polytechnic University, San Luis Obispo
21. CSU San Marcos
22. Sonoma State University
23. CSU Stanislaus

©2005 by Carnegie Mellon University

® CERT is registered in the U.S. Patent and Trademark Office

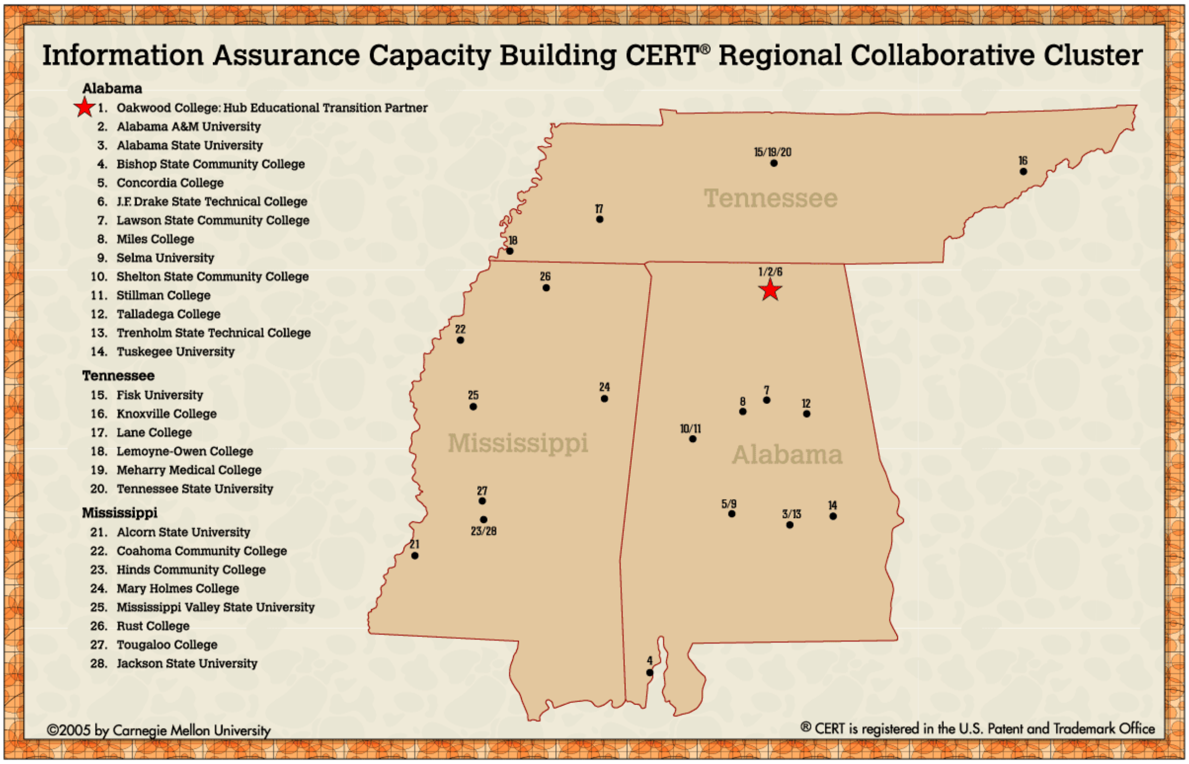
Appendix C: Texas Regional Collaborative Cluster



Information Assurance Capacity Building CERT® Regional Collaborative Cluster

1. Texas A&M University - Corpus Christi, Corpus Christi, Hub Educational Transition Partner
2. Alamo Community College District, San Antonio
3. Coastal Bend College, Beeville
4. Del Mar College, Corpus Christi
5. El Paso Community College, El Paso
6. Houston Community College, Houston
7. Howard College, Big Spring, TX
8. Huston-Tillotson College, Austin
9. Laredo Community College, Laredo
10. Midland College, Midland,
11. Mountain View College, Dallas
12. Northwest Vista College, San Antonio
13. Our Lady of the Lake University, San Antonio
14. Palo Alto College, San Antonio
15. Prairie View A&M University, Prairie View
16. San Antonio College, San Antonio
17. San Jacinto College (Central), Pasadena
18. San Jacinto College (North), Houston
19. South Texas Community College, McAllen
20. Southwest Texas Junior College, Uvalde
21. St. Edwards University, Austin
22. St. Mary's University, San Antonio
23. St. Phillips College, San Antonio
24. Sul Ross State University, Alpine
25. Texas A&M International University, Laredo
26. Texas A&M University – Kingsville, Kingsville
27. Texas Southern University, Houston
28. Texas State Technical College, Harlingen, Harlingen
29. University of Houston, Downtown, Houston
30. University of St. Thomas, Houston
31. University of Texas, Brownsville and Southmost College, Brownsville
32. University of Texas, El Paso, El Paso
33. University of Texas Health Science Center at San Antonio, San Antonio
34. University of Texas, Pan American, Edinburg
35. University of Texas, Permian Basin, Odessa
36. University of Texas, San Antonio, San Antonio
37. University of the Incarnate Word, San Antonio
38. Victoria College, Victoria

Appendix D: Proposed Southern Regional Collaborative Cluster



Information Assurance Capacity Building CERT® Regional Collaborative Cluster

Alabama

1. ★ Oakwood College: Hub Educational Transition Partner
2. Alabama A&M University
3. Alabama State University
4. Bishop State Community College
5. Concordia College
6. J.F. Drake State Technical College
7. Lawson State Community College
8. Miles College
9. Selma University
10. Shelton State Community College
11. Stillman College
12. Talladega College
13. Trenholm State Technical College
14. Tuskegee University

Tennessee

15. Fisk University
16. Knoxville College
17. Lane College
18. Lemoyne-Owen College
19. Meharry Medical College
20. Tennessee State University

Mississippi

21. Alcorn State University
22. Coahoma Community College
23. Hinds Community College
24. Mary Holmes College
25. Mississippi Valley State University
26. Rust College
27. Tougaloo College
28. Jackson State University

® CERT is registered in the U.S. Patent and Trademark Office

Appendix E: Partial Results of the 2004-2005 IACBP Faculty Participants

The past two years of the Information Assurance Capacity Building Program has resulted in the following developments, among others:

- Five new undergraduate courses:
  - Introduction to Information Assurance (Hampton University)
  - Beginning Information Assurance (Hampton University)
  - Computer Information Security (California State University, L.A.)
  - Information Security Management (California State University, L.A.)
  - Information Security (Oakwood College)
- Five new graduate courses:
  - Information Security (Texas A&M University, Corpus Christi)
  - Network Security (Texas A&M University, Corpus Christi)
  - Applied Cryptography (Texas A&M University, Corpus Christi)
  - Survivable Systems Analysis (Texas A&M University, Corpus Christi)
  - Advanced Information Assurance (Texas A&M University, Corpus Christi)
- Seven new modules added to existing courses
  - Undergraduate research (Texas A&M University, Corpus Christi)
  - Computer Literacy (Hampton University)
  - Computer Science I (Hampton University)
  - Software Design & Development (Hampton University)
  - “ID Protection” added into the courses “Intro to Computers,” “Data Structure II,” and “Operating System I” (Hampton University)
  - The general concept of “Security” added into “Operating System I” (Hampton University)
  - Artificial Intelligence (Texas A&M University, Corpus Christi)
- Six new degree options
  - Information Assurance graduate program for Computer Science students (Texas A&M University, Corpus Christi)
  - Master’s in Information Assurance (California State Polytechnic University, Pomona)
  - Professional MBA in Information Assurance (California State Polytechnic University, Pomona)
  - A.S. Degree in Network Administration and Security Management (Mount San Antonio College)

    - 2+2 Business Degree in Information Assurance (California State Polytechnic University, Pomona with Mount San Antonio College)
    - 2+2 A.S.-B.S. (Mount San Antonio College's A.S. degree in NASM will articulate to California State University, Fresno's BSIT - Bachelor of Science in Industrial Technology)
- Eight grant proposals
    - NSF Building Information Assurance Infrastructure (Hampton University)
    - NSF Federal Cyber Scholarship for Service Capacity Building grant proposal titled "A Regional Collaborative Cluster: Development, Dissemination and Adaptation of Information Assurance Survivability Curriculum" (California State Polytechnic University, Pomona)
    - NSF "Ethics Education in Computing: A Moral Development Constructivist Approach" (Texas A&M University, Corpus Christi)
    - CISCO (Texas A&M University, Corpus Christi)
    - CCLI A&I "Adaptation of a Computer Forensics Course" (Texas A&M University, Corpus Christi)
    - NSF SFS Collaborative Project: Capacity Building in Cyber Forensics Curriculum Development in CS and IT (Texas A&M University, Corpus Christi)
    - NSF Cyber Trust "Signature-based Network Intrusion Detection Using JESS" (Texas A&M University, Corpus Christi)
    - STC Center for Trusted Collaboration (Texas A&M University, Corpus Christi with Purdue University)
- At least 16 published papers
    - Partow-Navid, Parviz and Ludwig Slusky. "Evaluation of Campus Information Security." Paper presented to the Secure IT 2005 Conference, San Diego, CA, April 19-22, 2005.
    - Partow-Navid, Parviz and Ludwig Slusky. "IT Security in Pubic Organizations." In The Encyclopedia of Digital Government, edited by Ari Veikko Anttiroiki. Hershey, PA: Idea Group Reference, 2005.
    - Wilson, I.P. and M. Garcia. "Biometrics as a Cryptographic Key Generator." Paper accepted for publication at the Hawaii International Conference on System Sciences, January 4-7, 2006.
    - Dark, M., M. Garcia, Y. Qing, I. Ghansah, J. Chen, H. Lee, and C. Shing. "Adaptation of a State of the Art Computer Forensics Course." Paper presented to the 8th International Conference for Young Computer, Beijing, China, September 20-22, 2005.
    - Garcia, M., G. Gopal, J. Dick, P. Swaminathan, and K. Sunil. "Rule-based Intrusion Detection System Based on SNORT." Paper presented to the Network/Computer Security Workshop, Bethlehem PA, August 4-5, 2005.
    - Garcia, M., M. Dark, Q. Yuan, I. Ghansah, J. Chen, C. Shing, and H. Lee. "Adaptation of a Computer Forensics Course." Paper presented to the 6th International Conference on Information Technology-Based Higher Education and Training, Dominican Republic, July 7-9, 2005.

  - Aijaz, A. and M. Garcia. “Applications of Artificial Intelligence to Intrusion Detection.” Paper presented to the EuroIMSA 2005 conference, Grindelwald, Switzerland, February 21-23, 2005.
  - Young, L. and M. Garcia. “Using Recursion to Exploit Buffer Overflow.” Paper presented at IADIS International Conference Applied Computer 2005, Algarave, Portugal, February 22-25, 2005.
  - Balasubramanian, A., H. Pundir, V. Kankanala, and M. Garcia. “Enforcing Information Assurance Using Biometrics.” Paper presented to the 2005 ASEE Annual Conference and Exposition - Computers in Education Division, Portland, Oregon, June 12-15, 2005.
  - Dark, M., Q. Yuan, M. Garcia, I. Ghansah, J. Chen, and C. Shing. “Information Assurance Faculty Curriculum Development: What Works and What Doesn’t.” Paper presented to the Secure IT 2005 Conference, San Diego, California, April 19-22, 2005.
  - Manson, D., S. Corey, J. Fernandez, J. Blyzka, R. Farkas, P. Partow-Navid, and M. Garcia. “Beyond Bootcamps: A model for ongoing curriculum development collaboration for faculty attending an Information Assurance bootcamp.” Paper presented to the Secure IT 2005 Conference, San Diego, CA, April 19-22, 2005.
  - Fernandez, J., S. Smith, D. Kar, and M. Garcia. “Computer Forensics - A Critical Need in Computer Science Programs.” Paper presented to the Sixteenth Annual Consortium for Computing Sciences in Colleges South Central Conference, Lake Charles, LA, April 15-16, 2005.
  - Young, L., M. Aubuchon, and M. Garcia. “Recursions and Buffer Overflow in C++ Programming.” In Proceedings of the Symposium on Computing at Minority Institutions. (May 20-22, 2004), 82-88.
  - Allawali, F. and M. Garcia. “Computer Intrusion Detection Using Data Mining.” Paper Presented to the Texas A&M University System 2nd Annual TAMUS Pathways Student Research Symposium, October 14-15, 2004.
  - Durbha, K. and M. Garcia. “Threats and Facility Requirements in Physical Security.” Paper Presented to the Texas A&M University System 2nd Annual TAMUS Pathways Student Research Symposium, October 14-15, 2004.
  - Shroff, N. and M. Garcia. “Secure Socket Layer (SSL) Protocol: The Undisputed Heavyweight Champion for Web Site Authentication and Encryption of Transactional Data.” Paper Presented to the Texas A&M University System 2nd Annual TAMUS Pathways Student Research Symposium, October 14-15, 2004.
- 14 new certificate programs/workshops/symposia
  - 25% complete for 4011 Certification and began to map the 4012 objectives to courses they offer or plan to offer (the standards put forth by CNSS, Hampton University)
  - First IA Symposium (February 28, 2004, Hampton University)
  - Second IA Symposium (April 2, 2005, Hampton University

    - Plan for Third IA Symposium (April 4, 2006, Hampton University)
    - Second Annual Information Assurance Symposium (December 10, 2005, California State Polytechnic University, Pomona)
    - Certificate Programs in Information Assurance (California State Polytechnic University, Pomona with Mount San Antonio College and Cal State, L.A.)
    - Two-Day Workshop by IP3 (October 5 and 6, 2004, California State Polytechnic University, Pomona)
    - CISCO Security Bootcamp for Professors (December 13-16, 2004, California State Polytechnic University, Pomona)
    - Information Assurance Mini-Bootcamps (June 20-July 1, 2005, California State Polytechnic University, Pomona)
    - Participation in the “Secure IT 2005 Conference” (California State University, L.A.)
    - New three-course level one community college certificate: “Information and Operating System Security” (Mount San Antonio College)
    - Small business development workshops (Mount San Antonio College)
    - High school outreach initiatives (Mount San Antonio College)
    - K-12 and professional development initiatives (Oakwood College)
- Three new Regional Collaborative Clusters:
    - Mid-Atlantic Regional Collaborative Cluster - Hampton University in Hampton, VA, is a hub educational transition partner working with the SEI to build the capacity to teach information assurance at 22 colleges and universities in Virginia, North Carolina, Maryland, Delaware, and Washington, D.C.
    - Southern California Regional Collaborative Cluster - California State Polytechnic University, Pomona and Mount San Antonio College in Walnut, CA are hub partners that help build information assurance capacity at 23 universities in the Cal State system and 109 community colleges in California.
    - Southern Texas Regional Collaborative Cluster - Texas A&M, Corpus Christi is a new hub partner working to build capacity at community colleges and universities in Texas.
- One institution being designated a Center of Academic Excellence in Information Assurance (California State Polytechnic University, Pomona, 2005)

References

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

[CERT 06] CERT, Software Engineering Institute. http://www.cert.org/info_assurance/principles.html (2006).

[CSSIA 06] Center for Systems Security and Information Assurance. http://www.cssia.org/ (2006).

[Lipson 99] Lipson, Howard & Fisher, David. “Survivability—A New Technical and Business Perspective on Security.” *Proceedings of the 1999 New Security Paradigms Workshop.* New York, NY: Association for Computing Machinery, 1999. http://www.cert.org/archive/pdf/busperspec.pdf.

[Sledge 05a] 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)*. Atlanta, GA, June 6-10, 2005. Stoughton, WI: Printing House, Inc., 2005.

[Sledge 05b] Sledge, Carol A. *Report on Annual Regional Information Assurance Symposia* (CMU/SEI-2005-SR-007, ADA441807). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05sr007.html.

[Sledge 05c] Sledge, Carol. *Building Information Assurance Educational Capacity: Pilot Efforts to Date* (CMU/SEI-2005-SR-009, ADA441832). Pittsburgh, PA.: Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05sr009.html.

[Thomas 05] Thomas, Bill. “University Hubs Help SEI Spread Information Assurance Curricula and Methods.” *news@sei 8*, 1 (2005): 8-9. 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
(Leave Blank)

2. REPORT DATE
June 2006

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
Information Assurance: Building Educational Capacity

5. FUNDING NUMBERS
FA8721-05-C-0003

6. AUTHOR(S)
Carol A. Sledge, PhD

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2006-SR-007

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

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

This report is the fourth in a series describing the efforts by the Software Engineering Institute (SEI), and in particular those of its CERT® Program to increase the capacity of institutions of higher education to offer information assurance (IA) and information security (IS) courses. Other goals are to expand existing IA and IS offerings and to include IA and IS topics and perspectives in other courses. For each participating institution, these efforts are aligned with the focus of its involved academic department, current curriculum, and accreditation requirements. The report describes SEI activities for accomplishing its goals: participating in faculty capacity building programs funded by the National Science Foundation; creating and transitioning courseware, materials, and a newly created survivability and information assurance curriculum; and collaborating with key regional educational institutions. This report also presents four approaches the SEI has developed for its educational outreach in IA. The SEI applies these approaches as it works with all institutions of higher education, with a particular focus on minority-serving institutions and community colleges in the United States.

14. SUBJECT TERMS
information assurance education, information security education, regional collaborative cluster, capacity building

15. NUMBER OF PAGES
36

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL