Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Information Assurance Capacity Building: A Case Study

Naomi Falby*, J.D. Fulp*, Paul C. Clark*, R. Scott Cote*, Cynthia E. Irvine*, *Senior Member, IEEE*, George W. Dinolt*, *Member, IEEE*, Timothy E. Levin*, *Member, IEEE*, Matthew Rose*, and Deborah Shifflett*

Abstract – Despite an urgent need to protect information in computer systems critical to business and government, the inadequacy of many security products combined with over-marketing and overstated claims leaves information managers with nowhere to turn. Cyber security education is needed to provide a population of individuals who can make sound choices for the operation and acquisition of information protection. A prerequisite is an adequate population of educators. We describe workshops intended to help educators new to the area of Information Assurance. The multiple objectives are: to identify key foundational topics to educators, to teach lessons learned regarding topics difficult to convey to students, and to create a sense of community among Information Assurance educators.

Index terms – Information Assurance, Education

I. Introduction

Computer and network security are in a sorry state. One only has to read various trade articles to realize that many of the products available today are inadequate. For example, Frato writes [1]: "You won't find the answers by poring over vendors' marketing materials. Sure, you'll learn that deep packet inspection, the next generation firewall, makes decisions based on packet content. But you won't be told that this feature has been around for years, … You won't find the silver bullet that stops network attacks by active response, because the vendors can't provide it. Their protection, based not on allowing what's authorized but on stopping what's known, is in the wrong place." With the plethora of products currently available, it is difficult to learn how to secure systems and networks from books, the trade literature, journals, etc. A considerable amount of self-serving theory and development promotes new "solutions," which are doomed to failure *ab initio* for various reasons, for example, because they attempt to solve the halting problem [2, 3].

Why do such products exist and, further, why does anyone use them? Consider some possible answers. One may be that, the individuals and companies developing the purported "solutions" are charlatans [4] bent on fame and/or profit. Another explanation is that many vendors and researchers believe that the technologies being offered are sufficient to protect national and commercial infrastructures. This may be due to two factors: failure to recognize the true nature of the threat and lack of awareness of information assurance technology's ability to offer better, well conceived solutions. Hence the need for increased education in Information Assurance is clear.

Those who need education run the gamut from researchers through the general population of users. It is logical to assume that a prerequisite for strong programs in cyber security education will require knowledgeable teachers – ideally subject matter experts. Based upon this premise, we have been engaged, for the past seven years, in an effort to raise both the capacity and proficiency of the Information Assurance curricula at colleges and universities through IA education workshops.

This paper describes the most recent of those workshops, including the choices made regarding its content, organization, and results.

II. Background

In 1997, the Naval Postgraduate School held the first in what has become a series of gatherings by Information Assurance educators to focus on the problem of Information Assurance (IA) education. This was the Workshop on Education in Computer Security (WECS).

The first WECS meetings attracted an international group of IA educators. From the outset, each workshop has focused on a few particularly vexing areas in IA education and has included a considerable amount of group discussion, break-out sessions, and invited tutorials on unusual topics, as well as paper presentations.

* *Center for Information Systems Security Studies and Research, Naval Postgraduate School, Monterey, CA*
This material is based on work supported by the National Science Foundation under Grant DUE-0210762. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the sponsors.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

The *raison d'etre* of the workshops has been to serve educators who are active in IA pedagogy. Recognizing that each institution has a unique character and should tailor its program to meet institution-specific educational objectives, the intent was not to set standards or to dictate model curricula. Instead, the workshops provided a venue for information exchange and exploration of IA pedagogy. For example, at one WECS, considerable attention was devoted to the problem of keeping course materials current in a field with rapidly evolving technologies. The challenges of the IA educational community are exacerbated by the fact that, many new to the field lack the core historical foundations of IA upon which further understanding relies.

In 1999, the International Federation for Information Processing (IFIP) Technical Committee 11, Working Group 11.8 held its first conference in Stockholm, Sweden. Called the World Conference on Information Security Education (WISE), it was the result of many years of activity within IFIP TC 11, WG 11.8, and provided an expansive forum for collegial exchange [5].

In 2003, serendipitous circumstances allowed the WECS and WISE activities to be blended into a weeklong IA program. The workshop and conference were intended for teachers who were new to IA and needed help in getting started, for faculty who were starting to set up their IA curricula, and for experienced teachers who might benefit from the opportunity to exchange ideas about current technical topics and teaching approaches.

While the WISE conference retained its usual format, and that year had a theme focused on Critical Infrastructure Protection [6], WECS focused on IA capacity building and used a tutorial format. The innovations developed for WECS are highlighted in subsequent sections.

III. Workshop Participants

Program participants were composed of two groups: individuals selected to attend the WECS tutorials and subsequent WISE conference, and those who attended only the conference.

As a well-publicized activity of the IFIP, the WISE conference included the usual mix of presenters and participants. The papers presented were subjected to the standard academic peer review process.

The tutorials required much more attention in the area of participant selection, which will be discussed here.

A. Target Audience

The target audience of the workshop was college-level educators with responsibility for teaching curricula that are, or could be, related to Information Assurance issues. Through our sponsor, we were able to support each participant by providing: transportation, a food and lodging stipend, workshop materials as well as registration at the subsequent WISE meeting. Our sponsor provided support so that 20 scholarships could be offered to participants.

We noticed a rather uneven distribution of IA education venues in the U.S. Schools offering IA curricula are heavily concentrated in the Mid-Atlantic region and New England states, but there are far fewer in the Western states. For example, of the 50 Centers of Academic Excellence in Information Assurance Education, only 13 are in states West of the Mississippi, while 35 are located in the Eastern states [7]. Consequently, we put a special focus on institutions of higher education in the western states, while not precluding participation by colleagues in the rest of the country.

B. Participant Recruitment

Potential participants for the workshop were solicited using a number of vehicles including:

- Announcements and application packets sent to a list of colleges and universities in the U.S. West.
- Computing Research Association Newsletter
- Previous WECS participation lists
- All institutions represented in applications for participation in the National Science Foundation-sponsored Scholarship for Service program at the Naval Postgraduate School
- Publications in computer science and high tech areas
- Appropriate Internet web pages
- Registration with appropriate Internet search engines

Particular care was taken to ensure that underrepresented groups were made aware of this program. We contacted tribal colleges associated with the American Indian Higher Education Consortium (AIHEC), the historically and predominately black colleges associated with the National Association for Equal Opportunity in Higher Education (NAFEO), and the Hispanic Association of Colleges and Universities (HACU). Better representation of women was addressed through contact with the International Electrical and Electronics Engineers (IEEE) Committee on Women in Engineering (WIE) and the Association for Computing Machinery (ACM) Committee on Women in Computing as well as the CRA.

An application form based upon summer scholar programs sponsored by major government agencies was

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

created. It included sections for applicant facts, institutional demographics, and facts that contributed to a brief description of the program at the applicant's home institution. In addition, two letters of recommendation were required for each applicant: one from a colleague and the other from the applicant's department chair or equivalent.

C. Participant Selection

Participants were selected based upon application materials. Factors considered included:

- Faculty status in a college or university, or similar (e.g., industrial) education program
- Plans for or participation in an IA-related curriculum
- Statement of interest

These criteria permitted selection of participants with a high potential for success in workshop participation and IA education, where success depends not only upon technical proficiency, but also on communication and team building skills, and teaching abilities.

Due to limited funds for the tutorials, individuals from official IA Centers of Academic Excellence (IA CAE) were excluded. Our rationale was that, mastery of the topic would be a *sine qua non* for the IA CAE designation , viz., to paraphrase Webster [8], surpassing others in IA pedagogy, or eminent in a positive sense with respect to IA. Thus, IA CAEs should be less needy for introductory material on IA pedagogy.

The result was a diverse group. WECS participants came from Arizona, California, Nevada, Oregon, and Washington. Of the 20 tutorial participants, 13 were from community colleges, 5 were affiliated with universities and two were faculty members at four-year colleges. The group gender mix was 25% female, which is commensurate with the national occupational statistic for women in computer science in 2002 [9,10].

The WECS application materials required participants to explain how they were involved with under-represented groups. Responses showed a broad range of atypical student characteristics:

- Ethnic minorities
- Gender minority
- Native American
- Economically depressed
- First-generation college attendee
- Student with a disability
- Displaced homemaker
- Rural area
- Single parent
- Limited transportation
- Conflicting work schedule
- Those in retraining
- Military reservists and veterans
- Faculty peers with no IA knowledge

There was an overall positive explanation of how the department or institution was currently involved in out reach to under represented groups in their communities and extended areas. Participants were quick to explain current use of, and to suggest new ways to use, the pre-existing efforts. A few examples are industry-sponsored partnerships with high schools, training programs with local government, and student-success-oriented groups targeting specific underrepresented groups.

IV. WORKSHOP ORGANIZATION

The program format included three areas: tutorials, lab exercises, and working sessions. The objectives were: to help newer practitioners become knowledgeable about the basics of IA and IA pedagogy, to provide an opportunity for experienced practitioners to present new ideas for discussion, and to allow discussion of and potential development of solutions for point issues presented by the workshop.

WECS tutorial sessions were designed to educate participants about the fundamentals of Information Assurance and computer security and to improve their instructional capability in these areas. There were presentations and discussions of recent pedagogical and technical advances in the field. Finally, activities in the working sessions as well as informal exchanges encouraged creative interaction.

A. Tutorials

The goal of WECS was to broaden the IA knowledge base for attendees, and to provide an overview of pedagogical methods and techniques that have proven successful for teaching Information Assurance topics. It was organized to take place over a three-day period using a tutorial format.

After welcoming the participants the students watched a video entitled "Strategic Cyber Defense: Defending the Future in the Digital Domain" [11]. It depicts an imaginary cyber attack by an imaginary country named Kuracq on the US. The film was intended to provide motivation for the remainder of WECS. What followed was a mixture of talks and laboratory activities. At all times, participants were encouraged to ask questions and discuss the topic under consideration.
Material for the workshop was divided into four major categories:

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Pedagogy – The objective of pedagogy portions was to teach workshop attendees important concepts in Information Assurance that are sometimes overlooked
Examples – These lectures included technical demonstrations that provided attendees with examples of how difficult concepts can be conveyed to students. Despite the fact that some concepts are intuitively obvious to the cyber security expert, many ideas in IA are not necessarily easy for students to understand.
Laboratories – Our goal in the laboratories was to provide examples of the type of laboratory activities that are successful. We have been teaching computer security in our Computer Science curriculum since the early 1990's to students from a variety of curricula, cultures, and countries. As a result, we have learned through students' examination results, feedback, and experience which laboratory activities are most effective.
Discussion – To encourage interaction between participants, we reserved time for discussions during and after each event.

Table 1 provides a complete list of the WECS activities, in the order presented.

B. Conference

As the host institution for the World Conference on Information Security Education (WISE), we scheduled WISE to start on the day immediately following the WECS workshops. All WECS participants were enrolled in WISE with the objective of introducing the WECS group to a larger community of experienced Information Assurance educators. The benefits of WISE included:

- International – IFIP TC 11 WG 11.8 is international in scope. Thirteen countries and five continents were represented at the conference.
- Refereed papers reviewed by a 20-member program committee
- The conference had 62 registered attendees. In addition, NPS personnel attended many sessions.
- Activities to promote interaction

V. RESULTS

The size of the combined workshop and conference helped ensure considerable interaction among participants. As hosts, the NPS Information Assurance group, and the NPS students who assisted at the workshop made a significant effort to ensure that all attendees were fully engaged both in and out of lectures. The highly interactive format provided ongoing stimulation for the participants.

A. Participant Feedback

A questionnaire completed by WECS participants provided valuable feedback on the different modules within the tutorial sessions. There was consensus on several points:

- The three-day length of the tutorials was appropriate.
- The labs were the most helpful part of the tutorials.
- There is considerable interest in information on the topics of ethics, cyber law, and grant writing.
- Pedagogical materials for classroom use remain in short supply.
- Informal discussion groups were very useful.

The feedback received on individual units presented during the tutorial will permit improvements for future WECS conferences.

VI. CONCLUSIONS AND FUTURE EFFORTS

We observe that the periodic gathering and commingling of experienced and inexperienced practitioners enhances a sense of community among IA educators, fostering collaboration and dialogue among institutions offering courses and programs in Information Assurance. The net effect of the workshop has been to directly enhance the national capacity for education in Information Assurance as well as to extend the knowledge and expertise of IA to a range of participants that is more representative of the national profile.

A. Future Workshops

WECS includes a multi-year format intended to allow attendees to apply workshop concepts and return to the next workshop with experiential questions and insight. The experiences of 2003 participants will be presented in the 2004 workshop both through a survey and presentations.

In 2003, few NPS students attended WECS because it was held during a break between academic quarters. The 2004 WECS will be held during the academic quarter so that participants may be exposed to active working military students from around the world.

The presence and participation of NPS students will give a successful working example of how members from various groups can benefit from and flourish in an IA program. Many NPS military students pursue a Computer Science Master's degree although lacking an undergraduate degree in the field. They reflect ethnic and cultural diversity; and, for some, English is a second language

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

TABLE 1
CONTENT FOR THE WECS 2003 INFORMATION ASSURANCE WORKSHOP FOR EDUCATORS

Type	Title	Length (min)	Description and Comments
P-lecture	IA Pedagogy	40	This lecture was intended to provide a very high-level overview of Information Assurance pedagogy and emphasized many of the principles summarized by Saltzer and Schroeder [12]
E-Lecture	Passwords	50	This lecture provided examples of how material regarding the mathematics behind strong password selection can be conveyed to students.
E-Lecture	Encryption	60	Encryption can be very confusing for novice students. Here we gave examples from our experience in teaching the difference between symmetric vs. asymmetric cryptography; substitution (confusion) and transposition (diffusion), publicly scrutinized algorithms, the effect of key length, hash functions, and other facets of cryptography.
Laboratory	Passwords and Encryption	60	Participants were able to try hands-on laboratory exercises for the topics of passwords and encryption.
E-Lecture and Discussion	Malware	140	This lecture included several classroom demonstrations as well as more traditional lecture material and included discussion of viruses, Trojan Horses, and steganography.
E-Lecture	CIP and IA	30	Experienced IA personnel are urgently needed to assist with Critical Infrastructure Protection (CIP) [13]. This lecture gave an overview of CIP and its relationship to IA.
E-Lecture	Policies – DAC and MAC	60	The difference between discretionary and mandatory security policies is often confusing for students. This lecture provided insights regarding how to convey the concepts associated with MAC and DAC.
E-Lecture	Assurance	60	Motivation and approaches to assurance in secure systems was discussed with emphasis placed upon the constructive aspects of security [14].
Laboratory	DAC and CC Toolbox	60	This laboratory allowed participants to take a test run through laboratory exercises elucidating the notion of discretionary policies discussed in the morning. They also explored assurance by experimentation with the Common Criteria Tool Box [15].
Discussion	Challenges in IA instruction	60	This was a facilitated discussion of a wide range of topics in IA education.
P-Lecture	IA Textbooks	30	A review of available textbooks and criteria for selecting one appropriate to the target student body was discussed.
E-Lecture	Covert Channels	60	The types of covert channels: storage and timing, accompanied by a discussion of the disk exhaustion channel A demonstration of the covert channel laboratory used by our students followed.
P-Lecture	The Administrative Element of IA	50	Because one can loose sight of security objectives, e.g., protecting company assets, jobs, and sometime lives, this segment discussed non-technical aspects of security and their impact on the efficacy of the technical measures.
E-Lecture	Threat/Safeguard Tutorial Introduction	30	The objective was to increase understanding of system threats and vulnerabilities by focusing on the problem through an adversary's perspective. Emphasis was on being able to visualize an offensive attack in order to improve network security defensiveness.
Laboratory	Threat/Safeguard scenarios	120	Practical experience with some techniques used by adversaries allowed participants to appreciate the asymmetric nature of Information Assurance.
P-Lecture	Running your IA Lab	40	A discussion of the administration, logistics, and support issues surrounding the design and use of a laboratory for use in conjunction with Information Assurance Classes was facilitated.
Laboratory	Vulnerability Assessment	180	This was a footprinting and enumeration exercise with hands-on use of tools used in classes
Key	P- Lecture – Pedagogical Lecture; E-Lecture – Lecture with Example Demonstration		

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Acknowledgements: We would like to thank Daniel Warren, the workshop participants, and the Scholarship for Service students who assisted during WECS and WISE: Cassandra Carrillo, Vickie Galante, Jennifer Guild, Jim Guild, Natalie Stauffer, and Donna Stewart.

REFERENCES

[1] Frato, M., Security, *Network Computing*, **14**(26):46-39. December 16, 2003.

[2] Turing, A. M. On Computable Numbers with an Application to the Entscheidungaproblem. *Proceedings of the London Mathematical Society*, series 2, 42, pp. 230-265, 1936.

[3] Spinellis, D., Reliable Identification of Bounded-Length Viruses is NP-Complete, *IEEE Transactions on Information Theory*, **49**(1): 280-284, 2003.

[4] Cohen, F., The Seedy Side of Security, *Network Security Magazine*, Fred Cohen and Associates, August 1998, available at http://all.net/journal/netsec/1998-08.html.
Downloaded 7 March 2004.

[5] Proceedings of the IFIP TC11 WG 11.8 First World Conference on Information Security Education, Ed. L. Yngstrom and S. Fischer-Hubner. Kista Sweden, June 1999.

[6] Security Education and Critical Infrastructures, Ed. C. Irvine and H. Armstrong, Kluwer Academic Publishers, Norwell, MA, 2003.

[7] Centers of Academic Excellence, National Security Agency Central Security Service. http://www.nsa.gov/ia/academia/caemap.cfm?MenuID=10.1.1.2 Downloaded 10 March 2004.

[8] Webster's Revised Unabridged Dictionary, MICRA, Inc., 1998.

[9] Statistics and Data, U.S. Department of Labor, Women's Bureau, Frances Perkins Bldg., 200 Constitution Avenue, NW, Washington, DC 20210 http://www.dol.gov/wb/stats/main.htm
Downloaded 10 March 2004.

[10] 2001-2002, Taulbee Survey, Computing Research Association, http://www.cra.org/CRN/articles/march03/taulbee.html

[11] Debello, J. "Strategic Cyber Defense: Defending the Future in the Digital Domain", DARPA DVD produced by Four Square Productions, 2001.

[12] Saltzer, J. and Schroeder, The Protection of Information in Computer Systems, *Proceedings of the IEEE*, **63**(9):1278-1308, 1975.

[13] President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America 's Infrastructures The Report of the President's Commission on Critical Infrastructure Protection, United States Government Printing Office (GPO), No. 040-000-00699-1, October 1997.

[14] Irvine, C., Teaching Constructive Security, *IEEE Security and Privacy*, **1**(6): 59-61, 2003.

[15] Common Criteria Toolbox, SPARTA, Inc., Team, 7075 Samuel Morse Drive, Columbia, MD 21046 http://cctoolbox.sparta.com/cctb_page1.htm
Downloaded 15 March 2004.