Cooperative Information Assurance Capacity Building

Claude Turner, Harry Hochheiser, Jinjuan Feng, Blair Taylor, Jonathan Lazar, Azene Zenebe, Shiva Azadegan and Mike O'Leary

Abstract – ***The Maryland Alliance for Information Security Assurance (MAISA) is a consortium of 15 community colleges, colleges, and universities led by Towson University. By working collaboratively, we have been able to strengthen our information assurance education programs. We present our consortium, and describe some of our current projects and the effects that they have had on our information assurance education programs.***

Index terms – Consortia, Faculty development, Cooperation

I. Introduction

The limiting factor in the development of information assurance education programs has not been a lack of need or desire; for example, Joanne Sexton [1] directly asks: "Let's face it; virtually every computer science program wants to create a program in information assurance. Our computer science students actively seek courses in information assurance. We all know it's a profession with almost assured job security. So, what's stopping anyone?" In many cases the answer is a lack of resources. One problem may be that the institution does not have enough faculty with experience in information assurance; another may be that the institution does not have the capacity to offer the necessary courses. In many cases institutions have tried to solve this problem on their own; some have been successful, and others less so. In this paper we describe how a mixed group of community colleges, colleges and universities in Maryland have worked together to jointly strengthen their ability to provide information assurance education.

The Maryland Alliance for Information Security Assurance (MAISA) was formed by Towson University, a Center for Academic Excellence in Information Assurance Education. Today, MAISA is composed of five universities and ten community colleges, including two historically black universities. We work collaboratively to provide opportunities in

- Information Security Assurance curriculum development,
- Course and program sharing,
- Sharing articulation models between community colleges and universities,
- Networking with administrators and faculty involved with security training,
- Security training workshops, and
- Grant funding available for training and equipment

For more than five years MAISA has been very successful; we have been able to provide equipment, resources, and faculty development opportunities across the state. This approach has enabled us accomplish more together than we could have done separately. In what follows, we shall describe our consortium, some of our current and ongoing projects in information assurance education, and the benefits that this consortium approach to information assurance education development has provided.

II. Overview

The classical, canonical model for an institution skilled in information assurance has been advancement to the level of a Center of Excellence in Information Assurance Education (CAEIAE); see for example the discussion of Schweitzer, Humphries, and Baird [2] and the comments of Gene Spafford [3].

Narrowing our focus to curriculum development, there are a number of different approaches that an institution can take; following Perrone, Aburdene and Meng [4] they can be loosely classified as the development of a track, a single course, or a thread across multiple courses. Two of the authors describe how they developed a track in computer security at Towson University [5,6]. Liu and Leung [7] describe their approach at New York City College of Technology, while Boleng, Schweitzer and Gibson [8] describe the challenges developing IA skills at

Claude Turner: Department of Computer Science, Bowie State University, 14000 Jericho Park Road, Bowie, MD 20715 USA

Harry Hochheiser, Jianjuan Feng, Blair Taylor, Jonathan Lazar and Shiva Azadegan,: Department of Computer and Information Sciences, Towson University, 8000 York Road Towson, MD 21252 USA

Azene Zenebe: Department of Management Information Systems,Bowie State University,14000 Jericho Park Road, Bowie, MD 20715 USA

Mike O'Leary: Center for Applied Information Technology, Towson University, 8000 York Road Towson, MD 21252 USA

ISBN 1-933510-96-7/$15.00 © 2009 CISSE

the US Air Force Academy. Vaughn, Dampier and Warkentin [9] describe the program at Mississippi State. Dennis, El-Gayar and Streff [10] describe the model program developed at Dakota State while later Malladi, El-Gayar and Streff [11] present some of the lessons they learned; see also [12] and [13]. These institutions are generally large; see Sexton [1] for an example of the process at a small liberal arts college that is working towards CAEIAE designation

There are other ways to improve the delivery of IA education besides developing tracks or becoming a CAEIAE; this is the foundational goal of MAISA.

MAISA was founded by Towson University, the second largest university in the state of Maryland, the largest university in the Baltimore area, and the largest comprehensive university in the state with an enrollment of 17,272 undergraduate students and 3,839 graduate students. MAISA members include Bowie State University and Morgan State University, both Historically Black institutions. The other members are:

- Allegany College of Maryland
- Anne Arundel Community College
- Cecil Community College
- College of Southern Maryland
- Community Colleges of Baltimore County
- Frederick Community College
- Frostburg State University
- Garrett Community College
- Harford Community College
- Howard Community College
- Prince George's Community College
- University of Baltimore

We are not the only organization to have recognized the value of collaboration and cooperation in the development of IA expertise. Sledge, Manson, Berta, and Tsamitis [14] present the details of an information assurance capacity building program at Carnegie Mellon, a summer program that works with IA faculty at minority institutions. Falby, Fulp, Clark, Cote, Irvine, Dinolt, Levin, Rose and Shifflett [15] discuss the WECS workshops, aimed to develop faculty at non-CAEIAE institutions. Toderick, Mohammed and Tabrizi [16] present how they developed a remotely accessible computer laboratory that could be shared by a consortium of local community colleges, while North, George, Shujaee and Mumford [17] explain how a consortium of historically black institutions worked together to develop course modules in information assurance.

One of the foci of MAISA has been faculty development workshops; we have run more that 35 days of workshops to train MAISA faculty. These multi-day workshops have covered a wide range of topics, including Application Software Security (2005), Operating Systems Security (2005), Cyberlaw (2005), Applied Cryptography (2006), Computer and Network Forensics (2006), Identity Management and Identity Theft (2008), Wireless Security (2008), Smart Card Security (2008), and Web Application Security (2009).

Our work with MAISA is not confined to workshops; we have also been active in finding equipment and materials that could be used to support classes and curriculum in MAISA institutions. For example,

- Cisco donated over $880,000 worth of networking equipment that was used to create IA laboratories at MAISA member institutions.
- In December 2005, we received a textbook donation valued at $50,000 from Thomson Course Technology to further support Information Assurance education efforts at the University and at the participating members of MAISA.
- We received over $250,000 worth of system security tools from ISS which were then passed on to other MAISA institutions.

Recently we have begun work on three projects; the first "A Second Generation Faculty Development Program" has allowed MAISA to continue and expand our faculty development efforts in information assurance. Second is the project "Building Security In: Injecting Security throughout the Undergraduate Computing Curriculum" whose purpose is to develop a sequence of modules in computer security that can be inserted in the existing computer science curricula at participating MAISA institutions. Finally, Towson and Bowie are taking the lead to develop material and a web portal for MAISA and other institutions that describe how we can better integrate accessibility and usability into computer security and information assurance. We shall describe each of these ongoing projects in more detail.

III. A Second Generation Faculty Development Program

The project, "A Second Generation Faculty Development Program," began in September, 2007. Our goal is to create a second generation faculty development program in information assurance to train faculty across a range of Maryland colleges and universities. This training program has four primary components: (1) a seminar series to introduce security related topics to interested faculty; (2) an IA educators forum where more experienced educators can share their experiences teaching information assurance with their colleagues from other institutions; (3) a research mentorship program, where security researchers invite community college and junior faculty to work jointly with them on research problems in security; and (4) an externship program where advanced faculty work on joint research projects in government and industry. This is a multi-level approach to capacity building, aimed at faculty with differing levels of skill and experience.

The seminar series has let us continue to offer our faculty development workshops. These are typically two or three day workshops which we try to hold during breaks in the academic calendar- winter break, spring break, and the summer. Our focus has been on trying to find speakers from industry rather than from academia; we have had the COO of Aspect Security give a workshop, as well as speakers from General Dynamics Information Technology and the Chief Information Security Office for Towson University.

The IA educator's forums have been a place where faculty from different institutions can discuss topics of common interest. Rather than present material in a top-down, expert-led format, the IA educator's forums let us meet as peers.

The aim of the research collaboration component is to stimulate research among community colleges and non-research active faculty at four year colleges/universities through partnerships with research faculty at our research intensive institutions. In 2008, we solicited applications for three research projects, each pairing a research mentor with a research fellow; in 2009 we will be supporting three more projects.

The first project, "Emergency Evacuation and Rapid Depopulation Model with Secure Wireless Implementation Considerations," was carried out by a junior and senior research member of the Morgan State University faculty. The researchers present a clear and solvable problem statement. They identified the absence of an effective approach by the Federal authorities to link terrorist threats, strategy and available resources to fight terrorism and proposed two solutions to reduce any deficiencies in the current strategy. Their first approach is to develop a model of an optimal route to move people from train stations to the outskirts of urban areas in the event of a disaster. The second solution investigates the feasibility a secure wireless gateway to support a secure digital alerting and information management system.

The second research project, "Security Awareness, Ethics and Behaviors of College Students," was conducted by a senior research faculty from Bowie State University and a junior researcher from the Community College of Baltimore. This research is useful in identifying the level of awareness security among a non-random sample of 63 students taking an introductory computer security course at a Historically Black University and a Community College. The goal of this research was to use their findings to aid in designing future awareness training courses to reduce the level of risky behaviors among the students.

The third research project, "Securing Speaker Recognition Systems," is by a senior researcher from Bowie State University and a research fellow from Morgan State University. This research reports on difference measures in cross-channel data in speaker identification, and suggests ways to incorporate these differences in speaker recognition to help to improve speaker identification.

Each of these projects lasted for at least two academic semesters, or one academic semester and a summer. During the project, the research mentor and the research fellow met regularly, and both were supported by our project.

In 2008, we supported one faculty externship project "A New Class of Steganographic & Steganalysis Algorithms for Wireless Sensor Networks (WSN)." This project pairs one of our faculty from Bowie State University with Dr. Dwight Richards of RSoft Design Group, Inc. The research focuses on developing steganographic and steganalysis algorithms for the wireless sensor networks environment (WSN). The motivation for the research is attributed to the absence of the algorithms due to the challenges encountered in their development. The research team cites availability of limited power and limited computational capabilities of the nodes in the WSN environment as two of the research challenges.

IV. Building Security In

As computing faculty capabilities have not necessarily evolved to match the increased need for improved education in secure programming [18], a second project focuses on expanding earlier successful efforts in secure coding education [19] to a broader range of courses taught at diverse institutions. The "Building Security In: Injecting Security throughout the Undergraduate Computing Curriculum" project aims to develop, test, deploy, and disseminate security injections in pursuit of an eventual goal of establishing *security across the curriculum:* the inclusion of security concerns in classes throughout the undergraduate computer science and computer information systems curricula.

This project grows out of several years of experience with computer security and secure programming education at Towson University. Although experience with Towson's undergraduate track in computer security have been generally positive [5][6], optional tracks and related upper-level electives reach a minority of students, toward the end of their undergraduate careers. Our concerns that this approach may be "too little, too late" were consistent with a growing consensus that effective security education would require integration across the entire undergraduate computing curriculum [4][20].

Our security integration model uses targeted lab modules to introduce security concepts into existing courses. Known as *security injections,* these modules are designed as stand-alone, minimally-invasive assignments that can be integrated into existing courses with little or no disruption to existing curricula. Security injections are based on a common template, which includes background information describing the class of vulnerability under consideration, a description of the risk, a documented example of a vulnerability in an existing system, and strategies for avoiding the vulnerability. The core of each security injection is a student-completed checklist that can be used to assess the security implications of a small code example or system component. Discussion questions at the end of each exercise encourage reflection about the content.

Initial deployment of security injections focused on discussion of the “big three” secure coding issues: integer errors, buffer overflows, and input validation [21] in “pre-introduction to computer science” (CS0) and CS1 courses. Pre-and post-questionnaires aimed at assessing student awareness of security concerns indicated a significant increase in awareness for students who completed security injections (as opposed to control sections of students who did not) [19].

The “Building Security In” project extends upon this experience, expanding to include upper-level courses at a range of institutions. Courses to be added include the second semester of the introductory programming sequence (CS2), databases, networks, web development, and a general introduction to computer information systems (CIS0). As with CS0 and CS1, CS2 materials will focus on vulnerabilities associated with common programming errors. Injections in other courses will use the common template to cover security concerns that are relevant to specific course materials. Modules for the networks course will discuss protocol design and network configuration. Injections for databases will cover SQL injections, input validation, database design concerns, and access control. Similar issues may arise in the web development course, which will also likely discuss scripting attacks and specific web vulnerabilities. Materials for the introduction to computer information systems class (CIS0) will focus on familiar security concerns such as phishing and passwords, along with general concepts including risk management.

Although our initial results have been encouraging [19], our goal of demonstrating a broadly-applicable approach to computer security education requires adaptation to other, different institutions. Our “Building Security In” includes faculty members in diverse institutions in MAISA, including Towson, Bowie State, and community colleges from Baltimore, Harford, and Anne Arundel counties. Materials are being developed primarily at Towson and Bowie State, with faculty collaborators from the other institutions playing an active role in discussing content areas, deploying materials, and assessing results.

The resulting collaboration is critical for the success of this project. Adaptation of our approach to computer security education cannot, and should not, be forced upon uninterested and unmotivated instructors: such efforts would be doomed to fail. By involving faculty in the discussions, we are able to address concerns, adapt material to meet the needs of specific institutions, and build an engaged team of committed educators. Feedback from these colleagues has proven instrumental in improving the quality of the security injections and related materials that are the key products of this effort.

Flexibility in pedagogical approaches is a key component of this collaborative effort. The adaptation of security injections to meet the needs of individual classes is assumed. Although this limits our ability to conduct any sort of controlled assessment, the added value in terms of instructor buy-in and quality of revisions makes the tradeoff worthwhile. Taylor, Hochheiser, Azadegan and O’Leary [22] provide a more detailed description of project goals, background, and progress.

V. Integrating Usability and Accessibility in Information Assurance Education

The “Integrating Usability and Accessibility in Information Assurance Education” project focuses on a challenge that has emerged more recently to the IA community. Security mechanisms, no matter how robust the design is intended to be, cannot assure information security if they are not easily usable and accessible by the general public. However, a large number of existing security techniques and tools are developed without considering the actual needs and capabilities of the user. [23] It is not uncommon for people to stick important passwords to their monitors since they frequently forget them. The widely adopted visual CAPTCHAs are totally inaccessible for millions of users in this country who are visually impaired [24]. Despite the fact that the government requires accessibility in their computing systems [25], and the trend to require accessibility for private companies, the majority of faculty who teach security courses are not familiar with the topics of usability and accessibility, and do not incorporate these topics into their classes.

As an initial effort to address this problem, we started this project to build and continuously support a national community of faculty members to integrate usability and accessibility in Information Assurance (IA) education. It aims to connect faculty members in IA education through an online web portal that presents complete sets of educational materials, communication tools, and knowledge sharing mechanisms.

In order to achieve the community development goal, we are building an online web portal as a virtual space to support community needs, The primary audience of our community will be faculty members in the CS, IS, and MIS fields who are currently teaching or are interested in teaching information assurance courses. This includes faculty from diversified institutes ranging from top research universities to community colleges with two or three year programs. The experiences of the audiences will also vary significantly. Some faculty will be highly experienced in teaching IA courses; some will have extensive experience in teaching, but little familiarity with information assurance; others will be faculty who are just beginning their teaching career. We will reach the target audience through a number of dissemination mechanisms, including seminars, local conferences, small group meetings at major conferences, email lists, newsletters, and the most important of all: the online web portal.

The web portal will provide an open access virtual space for community members to communicate, learn, and share experiences. The portal will consist of three key components: a resource center, a bulletin board, and an open access teaching Wikipedia. The resource center will provide faculty access to the teaching materials developed in the first year of the project. There will be two sets of materials, one on usability integration in IA education, the other on accessibility integration in IA education. An online lecture series on each of the two topics will be available. The bulletin board provides a mechanism through which faculty can communicate with each other, share information, make friends, and form research collaborations. The open access teaching Wikipedia will provide a powerful online resource center to which faculty can contribute their own teaching modules, methods, scenarios, and any other valuable materials that they developed.

The web portal will be the essential component of this capability building project since it will allow us to bypass the obstacles of physical distance and reach a large body of faculty located in every state of the country. Compared to local training programs that incur significant travel and accommodation costs, the online community will provide faculty the opportunity to learn the important topics and improve their IA courses with minimum cost.

Online communities have the advantages of reaching large numbers of users who are located in dispersed areas, but they also have disadvantages such as lack of community identities, lack of trust among members, ineffective communication, etc. In order to overcome those disadvantages, we will hold several small group meetings at major CS, IS, and MIS conferences such as International Conference on Information Systems (ICIS), Americas Conference on Information Systems (AMCIS), ACM Conference on Computer Science Education (SIGCSE), and ACM Conference on Information Technology Education (SIGITE). These small meetings will tighten the ties among community members and help establish a more open and collaborative community environment.

The teaching material development activity will provide the initial resource for the newly formed community. The material development efforts are accomplished by joint efforts of the faculty at Towson University and Bowie State University. Through this process, faculty at Towson University who are conducting intensive research in usability and accessibility also help develop a faculty team at Bowie State University who can teach usability, accessibility, and IA courses and conduct research in the related fields,

We are also developing a research mentorship program, where security, usability, and accessibility researchers at Towson University and Bowie State University invite community college and junior faculty to work jointly with them on research projects. Each collaboration project will focus on one topic and will be led by a mentor who is an experienced researcher in that field.

Overall, the project structure ensures that faculty with different level of skills and background work in an integrated team and benefit mutually from the collaboration. The unique distribution method of the online web portal will enable a large body of faculty nationwide to access the lecture materials and improve their IA courses.

VI. CONCLUSION

The collaborations we have been able to create and foster with MAISA have benefitted a wide range of Maryland institutions, from research intensive CAEIAE institutions to participating community colleges. Though the impact from our current projects will not be completely felt across MAISA for some time yet, the impact from our earlier projects has been significant. For example, when reporting about our the effect of the first MAISA faculty development program (which ended in 2007), Howard Community College wrote "This sharing of best practices between MAISA colleagues has, and always will be, considered the most influential benefit derived from our MAISA membership" and "Without HCC's MAISA consortium involvement, we would probably not have been able to develop and deploy our new ELB-310 Lab, nor have evaluated and upgraded three of our five class curriculum teaching packages."

As another example, since becoming a member of MAISA, the Department of Computer Science at Bowie State University has developed seven Information Assurance related courses. It has established a network and security track in its undergraduate Computer Technology program, and a concentration in Information Assurance in its doctoral program. The department has also developed a dedicated computer and network security instructional lab. All of these activities were supported directly and indirectly by the department's participation in MAISA.

This consortium approach to capacity building has truly enabled us to accomplish more together than we could have separately.

VII. Acknowledgments:

Shiva Azadegan and Mike O'Leary were supported by the National Science Foundation under grant DUE-0416706.

Mike O'Leary, Claude Turner and Azene Zenebe were supported by the National Science Foundation under grant DUE-0723368.

Harry Hochheiser, Blair Taylor, Shiva Azadegan, Claude Turner, and Mike O'Leary were supported by the National Science Foundation under grant DUE-0817267.

Jianjuan Feng, Jonathan Lazar, Azene Zenebe, Claude Turner, and Mike O'Leary were supported by the National Science Foundation under grant DUE-0830865.

Thanks to AC Chapin, Patricia Gregory, Jack McLaughlin and our colleagues for their valuable contributions and feedback.

VIII. References

[1] Sexton (2008). Establishing an undergraduate information assurance (information security) program at a small liberal arts college, *Consortium for Computing Sciences in Colleges, USA*

[2] Schweitzer, Humphries, and Baird (2006). Meeting the criteria for a Center of Academic Excellence (CAE) in information assurance education, *22*(1), 151—160.

[3] Spafford, G. (2008). *Centers of Academic …. Adequacy*, Retrieved March 6, 2009 from CERIAS Blog Web Site: http://www.cerias.purdue.edu/site /blog/post/centers_of_academic_adequacy/

[4] Perrone, Aburdene and Meng (2005). Approaches to undergraduate instruction in computer security *Proceedings of the American Society for Engineering Education Annual Conference and Exhibition, ASEE.*

[5] Azadegan, Lavine, O'Leary, Wijesinha, and Zimand (2003). An Undergraduate Track in Computer Security, in *Security Education and Critical Infrastructures*, Cynthia E. Irvine, Helen Armstrong (Eds.), IFIP Conference Proceedings *253*, Kluwer, pp. 319—332.

[6] Azadegan, Lavine, O'Leary, Wijesinha, and Zimand (2003). An Undergraduate Track in Computer Security, in *Proceedings of the 8th Annual Conference on Innovation and Technology in Computer Science Education (ITiCSE-03)*, Thessaloniki, Greece, June 30 - July 2 2003, pp. 207—210.

[7] Li and Leung (2006). Development of a Security Education Program at a Minority Institution, *Proceedings of the 10th Colloquium for Information Systems Security Education*, University of Maryland, University College Adelphi, MD June 5-8, 2006.

[8] Boleng, Schweitzer and Gibson (2008) Developing Cyber Warriors, *The 3rd International Conference on Information Warfare and Security*: Peter Kiewit Institute, University of Nebraska, Omaha USA: 24-25 April 2008.

[9] Vaughn, Dampier and Warkentin (2004). Building an information security education program. *Proceedings of the 1st annual conference on Information security curriculum development*, pp. 41—45.

[10] Dennis, El-Gayar and Streff (2004). A model program in information assurance and computer security, *Issues in Information Systems 5*(11), pp. 97—102.

[11] Malladi, El-Gayar and Streff (2007). Experiences and lessons learned in the design and implementation of an Information Assurance curriculum, *IEEE SMC Information Assurance and Security Workshop, 2007. IAW'07*, pp. 22—29.

[12] Streff. and Zhou (2006). Developing and enhancing a computer and network security curriculum. *Journal of Computing Sciences in Colleges*, *21*(3), pp. 4—18.

[13] Figg and Zhou (2007). A computer forensics minor curriculum proposal *Journal of Computing Sciences in Colleges* 22(4), pp. 32—38.

[14] Sledge, Manson, Berta, and Tsamitis (2008). Five Years of Success: Some Outcomes of the Carnegie Mellon Information Assurance Capacity Building Program. *Information Systems Education Journal, 6* (61). http://isedj.org/6/61/. ISSN: 1545-679X. (Preliminary version appears in The Proceedings of ISECON 2007: §3543. ISSN: 1542-7382.)

[15] Falby, Fulp, Clark, Cote, Irvine, Dinolt, Levin, Rose and Shifflett (2004). Information assurance capacity building: A case study, *Proc. 2004 IEEE Workshop on Information Assurance*, US Military Academy.

[16] Toderick, Mohammed and Tabrizi (2005). A consortium of secure remote access Labs for information technology education. *Proceedings of the 6th conference on Information technology education* pp. 295—299.

[17] North, George, Shujaee and Mumford (2005). Collaborative information assurance capacity building at a consortium of colleges and universities, *Proceedings of the 43rd annual Southeast regional conference*, March 2005, pp. 18—20.

[18] Westervelt (2008). *Educators see secure coding training challenges, improvements*, Retrieved February 12, 2009 from Search Security.com web site: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1346086,00.html.

[19] Taylor and Azadegan (2008). Moving Beyond Security Tracks: Integrating Security in CS0 and CS1.*Proceedings of the 38th SIGCSE technical symposium on Computer science education*. Portland, OR.

[20] Pothamsetty (2005). Where Security Education is Lacking. *Proceedings of the 2nd Annual conference on Information Security Curriculum Development.*

[21] SANS Institute (2006). *New Report Identifies the Three Programming Errors Most Frequently Responsible for Critical Security Vulnerabilities and Security Incidents in 2006,* Retrieved February 12, 2009 from http://www.ssi-sans.org/resources/top_three.pdf.

[22] Taylor, Hochheiser, Azadegan, and O'Leary (2009). Cross-site Security Integration: Preliminary Experiences across Curricula and Institutions, *The 13th Colloquium for Information Systems Security Education.*

[23] Sasse, A. and Flechais I. (2005) Usable Security. In Cranor, L. and Garfinkel, S. (eds). *Security and Usability: Designing Secure Systems that People Can Use. O'Reilly*. 13-30.

[24] Sauer, G., Holman, J., Lazar, J., Hochheiser, H., and Feng, J. (2009, in press). Accessible Privacy and Security: A Universally Usable Human-Interaction Proof. Paper accepted for special issue of Universal Access in the Information Society Journal

[25] U. S. Government (2008). *Section 508*, Retrieved on March 10, 2008 from www.section508.gov