Partnerships between Universities and Community Colleges

Kamesh Namuduri, Assistant Professor, ECE Department, Wichita State University

Abstract

Wichita State University leads the Kansas Cybersecurity Consortium consisting of several community colleges within the state of Kansas, the Wichita Police Department (WPD), the Regional Computer Forensics Laboratory (RCFL) in Kansas City, Missouri, and regional industry. The efforts of this consortium are geared towards promoting education and training opportunities for professionals and increasing the number of trained professionals in this important field. At present, the consortium consists of seven community colleges that are either currently offering or planning to offer Associate (2-year) degrees in the Information Assurance (IA) discipline in the near future. The mission of this consortium is "to promote security awareness within the region through collaboration with local communities, community colleges, private industry, and law enforcement agencies and to pursue education, training, and research activities in information assurance and security disciplines". The partnerships range from sharing IA teaching materials and laboratory resources, to forming state-wide working groups and organizing state-wide education and training workshops. This paper provides the details of the activities being pursued by Wichita State University to bring cybersecurity awareness in our communities.

1. Introduction

Community colleges are a critical part of the educational system in our country, offering affordable education and training to millions of Americans [1]. There are twenty two community colleges within the state of Kansas which offer two year associate degrees in variety of disciplines. These community colleges serve the needs of the regional industries (aviation, electronics, and software among others) by providing the necessary basic technical education and training for the current and future workforce. Wichita State University (WSU) is one of the three major universities within the state of Kansas with an annual enrollment of 14,000 students.

WSU, in coordination with community colleges within the state of Kansas, the Wichita Police Department (WPD) and the Regional Computer Forensics Laboratory (RCFL) in Kansas City, formed an alliance (Kansas Cybersecurity Consortium) to increase avenues for partnership among the colleges and to increase security awareness in the local and regional communities. At present, WSU is working with the seven community colleges that are either currently offering or planning to offer Associate (2-year) degrees in Information Assurance in the near future.

The seven community colleges participating in the Kansas Cybersecurity Consortium collectively enroll more than 37,000 students in their associate degree programs in various disciplines. Johnson County Community College is the largest community college within the state of Kansas. Such a strong enrollment coupled with the proximity of these seven colleges to WSU provides significant advantages and opportunities for collaboration. Donnelly College located in Kansas City and Haskell Indian Nations University located in Lawrence (the two minority institutions in the state of Kansas) will be invited to participate in the consortium in the near future.

The mission of this consortium is "to promote security awareness within the region through collaboration with regional communities, community colleges, private industry, and law enforcement agencies and to pursue education, training, and research activities in information assurance and security disciplines".

The partnerships range from sharing Information Assurance (IA) teaching materials and laboratory resources, to forming state-wide working groups and organizing state-wide education and research conferences and workshops. As a lead institution, WSU takes the role of developing and designing the exemplary educational materials, courses, and curricula. WSU will also develop effective approaches and practices for providing technical education and training for current and future technical professionals in Cybersecurity and Forensics. Together, the participating institutions are working towards supporting the mission of producing more science and engineering technicians [2].

2. Partnership with the community colleges

WSU is partnering with the participating institutions, is currently in the process of articulating career pathways for students from two-year colleges to four-year institutions and to industry. The main objective of this partnership is to promote education and training opportunities for professionals and to increase the number of trained professionals in Cybersecurity. The second objective is to develop professional training programs for community college faculty and high school teachers pursuing technical education in Cybersecurity and Forensics. Through the partnership, WSU plans to establish and maintain cybersecurity education, research, and training programs at community colleges within the state of Kansas. The collaboration will also lead to increase security awareness within the region through collaboration with local and regional communities, community colleges, and law enforcement agencies. We plan to achieve these objectives by setting the following specific objectives to be implemented within the next few years.

(a) Develop, establish, and maintain a *common IA education and training program* (equivalent to National Training Standard for Information Systems Security or NSTISSI standards) at community colleges throughout state of Kansas. Degree programs focused on specific areas of concentration will be established at different colleges based on their individual strengths and local community needs.
(b) Design a *standard (2+2) curriculum* that allows a student with an associate degree with an IA concentration obtained at any Kansas community college to pursue a four-year degree program at WSU.
(c) *Promote partnerships* between WSU and community colleges within the state of Kansas. This will be achieved by sharing WSU resources (laboratory equipment, curricula, and faculty) with the community colleges.
(d) Promote collaboration among the community colleges within the state of Kansas. This will be achieved by promoting common and complementary curricula, for degree and certificate programs at different community colleges. Regular workshops organized by the Kansas Cybersecurity Consortium will provide avenues for community colleges for knowledge sharing.
(e) *Promote partnerships* between colleges, and private industry. This will be achieved through promoting collaborations and joint activities between community colleges, professional organizations such as the Information Systems Audit and Control Association (ISACA), The International Information Systems Security Certification Consortium (ISC2), and Information Systems Security Association (ISSA).
(f) *Promote partnerships* among WSU, community colleges and law enforcement agencies. This is achieved through collaborative research, and training activities between colleges, police departments within the state of Kansas, and regional computer forensic laboratory (RCFL). In addition, internship programs in RCFL, and other law enforcement agencies are being pursued for college students.
(g) *Provide professional development opportunities* to the faculty of community colleges through advanced training programs, collaborative research activities, and workshops.

The proposed activities lead to increased awareness of information security related issues in the community. The partnerships and knowledge sharing are expected to result in enhanced learning experiences for students and increased student retention rates in the area of Cybersecurity and Forensics for WSU and community colleges in the state of Kansas. We expect that students who graduate through the proposed career paths will pursue careers in Cybersecurity and Forensics disciplines in either Government organizations or industry.

3. Proposed Activities

Participants from the collaborating institutions met on several occasions during the past year and identified four tasks to be pursued and implemented within the next one year. The first task is to develop, establish, and maintain a common IA education and training program (equivalent to National Training Standard for Information Systems Security or NSTISSI standards) at the collaborating community colleges throughout state of Kansas. Specific areas of concentration will be established at different colleges based on their individual strengths and local community needs. The second task is to design a standard (2+2) curriculum that allows a student with an associate degree in an IA discipline obtained at any collaborating community college to pursue a four-year degree program at WSU in the same discipline. The third task is to develop professional development programs for community college faculty and K-12 teachers pursuing education in Cybersecurity and Forensics. The fourth task is to develop professional certification and training programs for security professionals in order to prepare them for the challenges and demands of the workplace. The four tasks are described below.

Task 1 - Common IA Education and Training Program

The first task is to establish a core body of IA knowledge for an associate degree program at community colleges. The proposed curriculum activities includes identification of this core body of knowledge, developing a set of core courses, enhancing the existing courses taught at community colleges by adding relevant IA modules, and building a laboratory facility for student training. Depending on the unique strengths of the community colleges, community colleges will be encouraged to consider developing new courses, and to enhance their existing courses. For each course in the core body of knowledge, we plan to develop necessary classroom instruction materials, laboratory exercises and projects that provide hands-on training. In the following sections, the proposed courses with their overall objectives, the major topics that will be covered and development plans will be described.

Information Assurance and Security. This course provides the student with insights into the technical aspects and key elements of information security. This knowledge will serve as a foundation for future study in this specific field. It adds an important dimension in the broader engineering/science curriculum. The overall goals in this course include the following: identifying the key principles of information security and learning how they work; learning how to critically analyze situations of computer use, identifying the issues, consequences and viewpoints; and providing security for information processing systems–secure operating systems and applications, network security, cryptography, security protocols, etc.

Computer Forensics. The purpose of this course is to provide students with the tools, and skill sets required to search a variety of computer systems (UNIX and Windows based workstations and desktops, Personal Digital Assistants) while insuring the integrity of the data contained on those systems. At the end of this course, students will be able to understand the core and legal aspects of forensics, and to collect evidence, discover information and determine its relevance to the investigation.

Secure Operating Systems. This course presents concepts of operating systems including process management, deadlocks, memory management, input/output, file structure, and system security. The objective of this course is to let students understand the fundamental principles of operating systems: process synchronization, scheduling, resource allocation, deadlocks, memory management, file systems, and security. Specific operating systems will be studied in depth. Programming assignments consist of modifications and enhancements to the operating systems studied in class.

Secure Database Systems**.** This course deals with the fundamental principles underlying relational database systems. Topics covered are: database design using E/R diagrams; relational data models; relational algebra; SQL; embedded SQL; database integrity; and security & authorization. The course includes a group project involving the design and implementation of a database application, and programming in embedded SQL.

Secure Computer Communication Networks**.** This course introduces ISO seven-layer network architecture to students. Network programming for the Internet environment including the basic concepts of TCP/IP; client-server paradigms; programming of clients and various types of servers; remote procedure calls; concurrency management; and interconnection techniques will be covered. It emphasizes the design principles that underlie the implementation of practical applications.

Information Assurance and Security Laboratory**.** The goal is to create a mirror of real world software development environments (in small, medium, as well as large organizations) by mimicking day to day business activities and simulating hacker attacks to test the operating systems, databases, applications, and other commonly used tools. Students will create various real world scenarios by configuring the systems in different topologies in order to detect vulnerabilities of the software and hardware systems. The purpose of this laboratory is to provide a hands-on facility for students to experiment with security related concepts and to develop new methods and tools for information security. Students will work in this isolated LAN environment (disconnected from rest of the world) to run security related experiments. Information warfare scenarios will be created in which users try to attack others' programs, files and confidential data. These experiments will be designed to detect vulnerabilities and weaknesses of software tools and applications that are currently used in real world applications. A "Honey pot" will be created to attract potential intruders in order to analyze and research their actions.

Task 2 - Standard (2+2) Curriculum Development

The (2+2) program is intended to provide a career pathway for students from two-year colleges to four-year institutions. The participating institutions and the region will benefit from this program in several ways. The program provides a clear strategy for students to pursue technical education in community colleges and continue towards a four-year degree program at WSU. It also provides an option for those students who start working in the industry immediately after obtaining an associate degree from a community college to pursue a four-year degree program, should they decide at a later stage. The 2+2 program also increases student enrollment in two-year degree programs offered at community colleges as well four-year degree programs offered at WSU. In the near future, implementation of this (2+2) program is also expected to provide a career pathway (2+2+2 program) for students from secondary schools to two-year colleges, and then to four-year colleges.

The participating institutions in the Kansas Cybersecurity Consortium recognize the importance of this initiative and started working towards developing this program in 2005. At present, WSU recognizes several courses in General Education, English, Mathematics, Social Sciences, Physics and Chemistry as equivalent courses to the courses offered at WSU. However, core courses in Computer Science and Engineering (for example, programming related courses) offered at community colleges are not currently recognized as equivalent courses at WSU. The curriculum mapping process requires WSU to look not only into curriculum issues, but also into ABET accreditation, community college faculty training, and laboratory infrastructure development issues among others. The process has already begun with a strong support from the administrators and faculty of the participating institutions.

Task 3 - Professional Development Workshops

Several meetings were held between the PIs and representatives of community colleges that led to the formation of the Kansas Cybersecurity Consortium. These meetings will be continued on a regular basis to facilitate communication among the participating members. State-wide bi-annual professional development workshops will be organized under the umbrella of Kansas Cybersecurity Consortium to facilitate interaction among the community colleges, the local community, industry and government agencies. The activities in the professional development workshop include the following.

- Best practices in curricula, courseware, and course materials
- Integrating current research topics into courseware
- Preparing hands-on laboratory exercises
- Preparing case studies based on real life incidents
- IT professional certifications such as CISSP, CISA, and CISM
- Designing the transition from community college to university (2+2) programs
- Integrating cybersecurity concepts and topics into other computer and information courses and training programs
- Recruiting students into degree programs
- Providing internship opportunities in government organizations
- Developing collaborations with local industry
- Understanding law, ethics and privacy issues

Task 4 – Professional Certification Programs

Professional certification programs provide professional development opportunities for technicians to enhance their skills and professional preparation to meet workplace demands. Cybersecurity and Forensics is a constantly changing discipline requiring the professionals to update their background on a regular basis. The US DoD Directive 8570.1, made official in August 2004 and implemented in December 2005, mandates that any full-time or part-time military service member, contractor, or foreign employee with privileged access to a DoD information system, regardless of job or occupational series, obtains a commercial information security credential accredited by ANSI or equivalent authorized body under ISO/IEC Standard 17024:2003. The directive also requires that those same employees maintain their certified status with a certain number of hours of continuing professional education each year [3].

Currently, professional organizations such as the International Information Systems Security Certification Consortium ((ISC)^2) and Information Systems Audit and Control Association (ISACA) offer certifications based on written examinations [4,5]. These certifications are widely accepted by industry as well as DoD as requirements for professional jobs in Cybersecurity and Forensics disciplines. The professional certification programs offered by the Kansas Cybersecurity Consortium will be geared towards providing the necessary basic training in Cybersecurity and Forensics disciplines. In addition, these certification programs will also prepare the participants for industry certifications.

4. Conclusion

This paper suggests that partnerships with communities are essential to bring awareness of cybersecurity with the region. It outlined the activities being pursued by WSU in collaboration with regional community colleges to achieve this objective.

References

1. Advanced Technology Education Centers: Partners with industry for a new American workforce, National Science Foundation document, 2004.

2. U.S. Department of Education, http://www.ed.gov/about/offices/list/ovae/pi/cclo/index.html

3. American Association of Community Colleges, http://www.aacc.nche.edu/

4. US DoD Directive 8570.1, https://www.isc2.org/cgi-bin/content.cgi?page=949

5. ISACA, http://www.isaca.org/

6. (ISC)^2, https://www.isc2.org/