Multi-disciplinary Approach to Cyber Security Education

Wendy A. Lawrence-Fowler
Department of Computer Science
The University of Texas-Pan American
1201 W. University Drive
Edinburg, Texas 78540
wfowler@utpa.edu

Abstract A multidisciplinary approach to cybersecurity education facilitates sound critical and analytic thinking and good communication. Students are introduced to a broader perspective and learn to think more openly and within alternative systems of thought. They are better prepared to recognize and assess assumptions, implications, and practical consequences.

Key words: cybersecurity education, computer security education; forensics education, multidisciplinary education in security, security

I. INTRODUCTION

“We live in a world where a nation’s security depends in no small part on the security awareness and practices of our agencies, firms, suppliers, schools, friends, neighbors, relatives and, well, all of us.”[1] The increasing number of security breaches and threats to personal, organizational, and national safety have created a focus on cybersecurity. Today’s security workload is outstripping the capacity of the current security workforce to meet the demand [2]. Personnel across all sectors are sought to fill the cyber workforce need[3]. A challenge is to identify the sorts of people and formal education that are needed to assure there is a highly skilled and creative workforce that can respond to the dynamic challenges of cybersecurity today and into the future. In response to the U.S. government/s recognition that “securing cyberspace is an extraordinarily difficult challenge that requires a coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector and the American people”[4], NIST introduced the National Initiative for Cybersecurity Education (NICE). NICE serves as a national campaign to increase cybersecurity awareness, education, careers, and training across all sectors. Education is used as the vehicle preparing the general public, creating the workforce of tomorrow and keeping today’s workforce up to date. To facilitate communication, NICE has developed the National CyberSecurity Workforce Framework (the Framework). The framework provides a common lexicon and a description of cybersecurity work in terms of categories and specialty areas. The categories group related specialty areas together. Each specialty area is defined by typical tasks and knowledge areas, skills and abilities (KSAs) required for work in the area[5].

For technology programs within educational institutions, emerging fields of study and practice in cyber security computer forensics, network security, software security, and critical infrastructure protection are increasingly important areas of interest [6]. The framework serves to guide curriculum decisions for both formal and informal education in cybersecurity.

This paper proposes that taking a multidisciplinary approach to security and more particularly cyber security results in graduates who can think more openly and within alternative systems of thought. They are able to recognize and assess assumptions, implications, and practical consequences.

II. CONTEXT FOR THE APPROACH

In 2007, The University of Texas – Pan American established an Intelligence Community Center of Excellence (IC CAE) in National Security Studies Program in collaboration with the U.S. Intelligence Community and funding from the Office of the Director of National Intelligence (ODNI). The purpose of the Center is to assure that professionals in the next generation of Intelligence Community are prepared with the appropriate skills and breadth of knowledge to be leaders in the national security challenges in the 21st century.

Focusing on the breadth of knowledge required to lead and recognizing that solutions to the current challenges in security demand the integration of human and technical resources, the UTPA IC CAE uses a multi-disciplinary approach to achieve substantial synergies in information assurance and analysis, risk assessment, management and leadership, as well as the application of technology. The IC CAE leads the discourse on national security across campus, identifying specific needs associated with bridging disciplines. To that end, the IC CAE manages an interdisciplinary Global Security Studies and Leadership Program (GSSL) with an undergraduate minor, a graduate certificate and a Master’s degree in Interdisciplinary Studies (MAIS). Its near-universal reach across the university curriculum is ambitious because it articulates skill and knowledge sets that reside in many of UTPA’s departments. Existing courses are taught by current faculty in established departments. For example, a graduate level course in Computer
Security and Forensics in the Department of Computer Science is part of the core technology competency courses in the MAIS. When the course is offered, students in the course come from not only the MAIS, but also Masters programs in Computer Science (MCS) and Information Technology (MSIT). While originally designed with a curriculum targeting a computer science audience, the content is delivered to take advantage of the synergies in understanding that can arise with analytical thinking and communication of diverse perspectives of a multidisciplinary audience.

III. THE GLOBAL SECURITY STUDIES PROGRAM

A. Overview of Master’s of Interdisciplinary Studies (MAIS)

The MAIS degree prepares students for careers in Intelligence and National Security through focus on advanced research, effective cross-discipline team communication, and critical analysis. Given that jobs in government or private industry often require multidisciplinary cooperation, the GSSL MAIS prepares students to work with people from different backgrounds, abilities, and knowledge bases. This approach assures that students have the opportunity to gain the perspective of and proficiency in multiple disciplines, preparing them for careers in national security.

The program engages students and faculty in five of the five Primary Critical Skill Sets/Competencies areas of specialization: Information Technology Specialists, Political / Economic Specialists, Language Specialists, Threat Specialists, Scientific/Technical Specialists. A number of general competencies for intelligence professional areas are also addressed: Analysis, Analytical Reasoning, Critical Thinking, Communications (oral and written), Research, developing rational conclusions and alternative solutions from ambiguity and limited data sets[7].

B. MAIS Curriculum

The GSSL MAIS consists of 36 semester hours of study, including a 12 hour core sequence, a 15 hour concentration in interdisciplinary studies and a 9 hour technical competency sequence. Through the core sequence the students learn how skill sets relate to the global context of intelligence and security work. The courses address competency skill areas including advanced research, problem solving, critical thinking, technical writing, and leadership. The core courses consist of Global Security, Open Source Research, Interdisciplinary Research and Analysis, and a practicum in Global Studies Security Studies. The interdisciplinary sequence addresses critical competencies required to understand the globalization of communication, societies, cultures, governments, businesses, and technology. The required courses include Culture and Communication, International Management, Cross Cultural Psychology, and Statistics.

The technology competency sequence provides students with the essentials of information technology and computer systems with a focus on information security. The three course sequence includes Information Security, Principles of Information Technology Systems, and Cyber Security and Forensics [7,8]. The first course is offered by the Department of Computer Information Systems located in the College of Business. The second two courses are taught in the Department of Computer Science in the College of Engineering and Computer Science.

IV. CYBER SECURITY AND FORENSICS COURSE FOR MULTIDISCIPLINARY AUDIENCE

Using a variety of learning resources, the Computer Science course in Cybersecurity and Forensics introduces the foundations of cybersecurity and cyber forensics theory, policy and application. The goal of the course is to assure that students gain an understanding of the breadth and depth of cybersecurity and cyber forensics in both abstract terms and in the context of real systems. Readings, lecture, discussion, and thought experiments [9] are used to introduce the underlying formalisms and technologies in computer science that address challenges and potential threats to confidentiality, integrity, and availability. A laboratory component reinforces formalisms and technologies introduced in lecture and discussion. The labs support understanding through direct experience in applying knowledge in new situations [10,11,12]. Students are exposed to different types of tools, techniques, and procedures, as well as policy and legal issues and develop skills in the reduction of theory to practice and abstraction of practice to theory.

A. Course Objectives

Upon completion of the course, students are expected to (1) understand the basic theory and concepts of cyber security and privacy including policies, models, and mechanisms; (2) understand ethics, legal issues, and human factors associated with cyber security and forensics; (3) understand security vulnerabilities and be able to describe threats and risks; (4) be able to explain best practices in giving access to systems and networks and implement proper authentication techniques; (5) be familiar with cryptographic techniques, asymmetric key algorithms, and create certificates; (6) describe the requirements for a cyber forensic investigation and demonstrate an understanding of tools, techniques and procedures; and (7) be conversant in current security related issues in the fields of cyber security and cyber forensics.

B. Course Topics

The course begins with an overview of the security problem followed by an introduction of fundamental tools and techniques for addressing security. After providing a broad introduction to security, the course focus shifts to forensics. Course topics include: confidentiality, integrity and access policies; information flow and content (encoding and entropy); cryptography and ciphers; network security; malicious logic, vulnerability analysis; strategic planning for security; law and legal issues; volatile and persistent data; forensics first responder activities; and hacking. Strategic planning for security is introduced as a scaffolding to provide a real-world context and supports the creation of connections between security topics.
C. Laboratory Component

The laboratory component of the course gives students practical experience with the concepts introduced in lecture and discussion. Each lab is designed so that students experience working with real world tools and real world problems. A broad array of commercial hardware and software, and open source tools are provided to develop solutions for problem based challenges involving confidentiality, integrity, access, and trust. Students identify and disable network attacks. They find hidden information, and they conduct forensic investigations using a systematic approach to evidence identification, preservation, analysis, documentation, and presentation following acceptable legal procedures and laws of evidence[10]. Additional lab exercises involve secure system design using covert channels and robust queues. [13].

Lab exercises are completed by interdisciplinary teams to encourage transfer of understanding and perspective across the spectrum of divergent bodies of knowledge held by course students and to address varying levels of comfort and skill in using technology.

D. Assessment Techniques Used

Substantive and formative evaluations were given to both assess students learning and to help in making adjustments to content delivery. Students were given weekly assignments that included a set of readings and at minimum one deliverable. Deliverables varied by week, but consisted of one or more of the following: 1) short responses to issue specific questions used to measure understanding of the lecture and reading assignments, 2) lab results along self-assessment of success, and suggestions on improving the lab, 3) short essays on how a reading relates to past, current, or future experiences in global information security, 4) contribution to a lexicon for security, 5) identification of a resource and explanation of its value. The time in lab provided additional opportunities to gather feedback about content delivery and student learning.

Two larger learning exercises served as exams. The first was given midterm. Students were given two questions that required them to research specific security models and discuss their application. A third question served as a thought exercise requiring critical thinking and synthesis. The second served as a final and gave student the opportunity to choose one of two challenges. In the first challenge students were to build a forensic tool kit from existing open source resources and write a comprehensive user’s guide on when, how and why to use each tool in acquisition, analysis and presentation during a forensic investigation. In challenge two, students were directed to read Cliff Stoll’s book “The Cuckoo’s Egg” and write a 7 to 10 page response to one of three prompts. Each of the prompts required analysis, synthesis, critical and creative thinking.

Finally, students completed UTPA’s standard Student Evaluation of Teaching Form. Students were encouraged to submit comments in the section with open ended questions.

V. Discussion

Computers, the Internet, e-mail, wireless technology toys, and social networks are pervasive and a ubiquitous part of everyday life. The growth in digital details that are created, captured, and stored in more places than most people realize is exponential as is the growth rate of crimes in which cyber technology is the instrument of, the target of, or by its nature, the location where evidence is stored or recorded. The number of security breaches and threats to personal, organizational, and national safety and the increasing costs of security breaches have created a focus on cyber security[5,14,15,16] and a demand for qualified security professionals in both the private and the public sector[4,7]. Academic institutions respond by offering new courses in cyber security [16] and forensics [10].

A. Challenges to Leverage Potential Synergy

When the Cyber Security and Forensics course was chosen for the GSSL MAIS technology sequence, the delivery was designed as an elective course in the Master’s of Computer Science and the Master’s of Science in Information Technology (MSIT) programs offered by the Department of Computer Science. Students were expected to be familiar with, operating systems, data structures, programming languages, software application programming and hardware and had typically completed an advanced networking course. The course took a breadth first approach to introducing the fundamentals of computer security and forensics. Students experience theoretical concepts and their implementation. Reflective learning exercises were designed to empower students to link prior knowledge with new knowledge and develop a deep understanding of the complexity of cyber security and forensics theory and practice.

However, with the inclusion of this course in the GSSL MAIS, the demographic profile of students taking the course changes radically. Less than 3% of the students have undergraduate degrees in computer science and are pursuing a Master’s degree in Computer Science. The remaining 97% of the students’ program affiliations are split fairly evenly between the MSIT and the MAIS. Yet, of this group, only 8% have formal undergraduate training in information technology.

The new demographic includes students who have undergraduate degrees in accounting, computer science, criminal justice, early childhood education, economics, graphic design, information technology, political science, psychology, and sociology. The majority of MAIS students move directly from an undergraduate education in social and behavioral sciences to the MAIS graduate program. Similarly, a number of the MSIT students do not have formal backgrounds in computer science or information technology, but they find themselves working as professionals in information technology. Fortunately many of these students have extensive experience in either networking or management information technology systems. On occasion the class includes a Chief Security Officer from a banking institution or local government agency. This demographic shift among the students taking the course presents a number of challenges to the traditional delivery.

Recognizing that the essential body of knowledge for the domains of security and forensics is broadly distributed and include deep subdomains, the first challenge is to modify the course delivery to take advantage of the diversity in the new
demographics body of knowledge. Given the IC CAE program goals, the five Primary Critical Skill Sets [5,6], and the UTPA GSSL program goals and curriculum, an approach to the topics is designed that recognizes that security issues do not rest solely in the domains of Computer Science and Information Technology[18].

Just as NICE has developed the Framework at the national level to provide a common lexicon for understanding categories and specialty areas for education of a cyber workforce, the diversity in students’ program of study in this class demands the establishment of a common lexicon in security and forensics. This supports effective communication and facilitates sharing of perspectives and knowledge across disciplines. Students use a forum to provide profiles, including their backgrounds and expertise; their knowledge areas, skills, and abilities (KSAs). A wiki serves as a dictionary for terms and concepts. A second wiki serves as a repository for student contributed resource materials. These wikis create a framework for growing the Essential Body of Knowledge (EBT) [19]. Thus the diversity of academic training, perspectives and experience means that students are exposed to the breadth of knowledge that professionals should know to be conversant in the field of cybersecurity and more generally security. Students, at minimum, know the key concepts and terms to perform their work functions in security and they gain, at least, a basic familiarity with all of the key terms and concepts in the EBT [19].

Thought exercises are used throughout the lectures to provide an opportunity for students to think independently, discuss their thoughts in pairs, and share their ideas with the class. This think-pair-share approach also serves as the basis for work outside of class. Students reflect on concepts and present their thoughts on forums or in the form of short essays. These reflections serve as the basis for conversation and the opportunity to elaborate on ideas. This approach increases personal communication that is necessary to process, organize and retain ideas [20]. The approach takes advantage of the students’ diverse knowledge base to expand individual perspectives on security and forensics topics.

The diversity among the students’ skill levels in the use and the understanding of computing environments confirmed that labs, originally designed to expose students to the concepts introduced in lecture and discussion are too complex. The labs are modified so that students with minimal background in computing are able to complete the exercises and gain conceptual insight. In addition, interdisciplinary teams are created where each team has at least one individual with a strong background in information technology to assure success. The mix of team KSAs reinforces the development of strong analytical thinking and good communication.

Finally, there is strong interest and investment in information security at the institutional level. Taking advantage of the human capital resources in Privacy and Security and in the Division of Information Technology, Subdomain experts in network security and forensic investigation provide class and lab instruction and guidance. The University’s Chief Security Officer along with recognized security experts from the health industry and intelligence community introduce strategic planning for security.

VI. CONCLUSION

This paper describes a Computer Science course in Cyber Security and Cyber Forensics offered at UTPA. The challenges of offering this course to a multidisciplinary audience lead to changes that leverage the diverse student knowledge base. During the course students learn, practice and gain understanding of concepts and develop the technical and leadership skills required of cyber security professionals. Hands-on lab exercises facilitate understanding of difficult concepts and procedures. Using both commercial and open source tools provides a rich environment. Using interdisciplinary teams facilitates the exchange of knowledge and understanding. Students see how complex the issues in cyber security and forensics are. Students gain an appreciation for true multidisciplinary nature of the field.

ACKNOWLEDGMENT

I would like to recognize Jennifer Garcia Avila for guiding us through EnCase, Ramon Herrera for providing expertise in network security Joe Voje for providing a strategic view for security, Dr. John Abraham for access to resource materials, Jeremy Miller in implementing many of the hands-on labs and the UTPA IC CAE for coordinating the 2012 Cyber Security Symposium.

REFERENCES


