3-2014

Roadmap for Graduating Students with Expertise in the Analysis and Development of Secure Cyber-Systems

Ann Q. Gates
University of Texas at El Paso, agates@utep.edu

Salamah Salamah
University of Texas at El Paso, ISALAMAH@UTEP.EDU

Luc Longpre
University of Texas at El Paso, longpre@utep.edu

Comments:
Technical Report: UTEP-CS-14-28

The University of Texas at El Paso
Department of Computer Science
Roadmap for Graduating Students with Expertise in the Analysis and Development of Secure Cyber-Systems

Ann Q. Gates
Salamah Salamah
Luc Longpré

1. Introduction

Due to the rapid expansion and reliance on the global Internet for day-to-day functions of individuals, organizations, governments, and industry around the world, cyber-security has emerged as an essential component of computing curricula. Today, software systems of large sizes and high complexity control almost all aspects of our lives. These systems play an integral role in the operation of larger systems used for defense, energy, communication, transportation, and manufacturing. Lack of attention to security and incorrect functionality can have devastating consequences including loss of life and major financial costs.

It is essential to train and produce a workforce that is capable of developing reliable, secure, and correct software systems. To address the regional and national need for software engineers and computer scientists capable of developing advanced, complex, robust, secure, and reliable systems for government and industry, the Department of Computer Science at the University of Texas at El Paso (UTEP) is offering a sequence of courses in Secure Cyber-Systems for both the Bachelor of Science in Computer Science (BSCS) program and the Master of Science in Software Engineering (MSSwE) Program. A specialized track in Secure Cyber-Systems (SCS) has been added to the 2014 undergraduate and graduate catalog. The vision of the new curriculum is to educate students to meet the expanding need for a workforce capable of taking a disciplined, process-oriented approach to the analysis, development, and deployment of complex secure systems of the 21st century. Both the BSCS and the MSSwE programs at UTEP are designed to prepare professionals, specifically, with the *engineering management* and *systems verification and validation* skills needed to develop reliable, complex systems.

In an attempt to address that regional and national need for expertise in cyber-security, the Computer Science department has set the following **goals**: (1) to increase the number of qualified students who complete the Secure Cyber-Systems (SCS) tracks at UTEP; (2) to graduate students who can enter the workforce with the ability to transfer state-of-the-art cybersecurity techniques and approaches into practice; (3) to place students in positions that utilize their knowledge and capabilities in cybersecurity.

The effort takes advantage of several innovative approaches to meet its goals. Recruiting will target qualified U.S. citizens with an emphasis on individuals from under-represented groups including females. UTEP has a significant history of attracting, supporting, retaining, and graduating minority students, in particular Hispanics who are first in their family to graduate and nontraditional students in STEM fields through the use of research-based approaches to student development.

Need. Modern society is intensely and irreversibly dependent on software systems of extraordinary size and complexity. This includes software systems in domain areas such as defense, energy, communication, transportation, and manufacturing. Additionally, society's use of the internet has moved from a luxury into a necessity. The number of internet users has increased from 360 million to over 2 billion between 2000 and 2010 [1]. Government agencies such as the Department of Defense (DoD) and the Department of Homeland Security (DHS) rely heavily on the use of software systems and cyberspace. For example, the DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe [1].

Our reliance on computer and software systems makes it is imperative that these systems operate correctly in terms of functionality, reliability, and security. Lack of security or incorrect functionality can have devastating consequences including extreme financial losses or even human fatalities. Still, software systems continue to exhibit errors and vulnerabilities and are regularly subject to attack and compromise. Attacker actions, when successful, can result in severe impacts and losses for the organizations that build, deploy, and operate these systems, as well as the business partners and customers who use them.

Throughout our nation and the world, there is an increased focus on the areas of secure software engineering and cyber-security. Because much of what we do is controlled and maintained by computer systems, cyber-attacks that threaten the integrity of these systems represent a major concern. A 2010 National Security Strategy developed by the White House states that [2, p.27]:

1. Cyber security threats represent one of the most serious national security, public safety, and economic challenges we face as a nation.
2. The very technologies that empower us to lead and create also empower those who would disrupt and destroy.
3. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient.

In order to counter cyber threats, the White House, DoD, and DHS continue to develop strategies that aim at producing a workforce capable of ensuring the integrity and reliability of the major cyber-physical systems the nation depends on. Thus, a key part of DoD's strategies for operating in cyberspace, is to "leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation." [1, p.5].

2. Background

UTEP is a major regional university serving a large, bi-national, bicultural population on the U.S.-Mexico border. UTEP is the second-oldest academic component of the University of Texas System and ranks among the top 25% of universities in Texas in terms of research expenditures. With a current population of approximately 700,000, El Paso is the fourth largest city in Texas. It is spread along the U.S.-Mexico border. Across from the border is Ciudad Juarez, a city with a population of around 1.3 million. The population of El Paso is estimated to be almost 81% Hispanic, and over 50% of El Paso's households speak Spanish as the language of preference. The University's ethnic composition reflects that of El Paso's population; more than 80% of UTEP students are from El Paso County and commute daily. In fall

2012, enrollment reached 23,003 with 77% of those students being Hispanics. UTEP is the only doctoral/research-intensive university in the U.S. with a student population that is majority Mexican-American.

The El Paso area is home to a number of military, intelligence, and law enforcement communities. Fort Bliss, White Sands Missile Range, Biggs Army Airfield, Holloman Air Force Base, and the El Paso Intelligence Center (EPIC) are all based in the region. Over 15 different government agencies are currently represented at EPIC.

UTEP's Department of Computer Science (CS), which has been accredited by ABET's Computer Science Accreditation Board since 1986, has 15 tenured or tenure track faculty members, two research faculty members, and one clinical faculty. The department offers a Bachelor of Science in CS (BSCS), a Master of Science in CS (MSCS), a Master of Science in Information Technology (MSIT), a Master of Science in Software Engineering (MSSwE), and Ph.D. in CS.

UTEP's research projects in the areas of border security and defense are enhanced by its unique location on the U.S.-Mexico border and a wide range of border-related research and educational programs on campus and in the region, including the Department of Homeland Security (DHS) funded National Center for Border Security Initiatives (NCBSI) and the Regional Cyber and Energy Security Center (RCES). In addition, the White Sands Missile Range (WSMR), the largest military installation in the U.S. and located 45 miles north of El Paso, houses projects funded by the Army, Navy, Air Force, Department of Defense, and NASA. Research in the CS department centers on the following main areas: computer science theory and its applications, software engineering, human-computer interaction, intelligent systems, and high performance computing. In addition to developing various security protocols, the computer science theory group involves many students in research related to privacy protection. The software engineering group has a focus on software assurance and formal verification. The high performance systems group investigates the design of systems that are robust to a wide range of operating conditions. The human-computer interaction group investigates communication mechanisms that minimize human error. The intelligent systems group investigates risk analysis, automated surveillance and decision-making in adversarial and cooperative settings.

UTEP was designated as a National Center of Academic Excellence in Information Assurance Education (CAEIAE) in 2010. The department offered a number of courses containing Information topics and also offers a graduate certificate in Cyber-Security. In addition, UTEP is currently seeking a designation as an NSA Center of Academic Excellence in Cyber-Operations. The required content (knowledge units) for this designation maps to the learning outcomes of the courses that make up the Secure Cyber-Systems tracks of the BSCS and MSSwE programs. The curriculum is described in more detail below.

To support research and the specialized curriculum, UTEP has invested in facilities that include the acquisition of hardware and software necessary for teaching and conducting research in the areas of security, reliability, and safety of real-timed embedded systems. The CS department currently has an academic lab and a research lab - **R**eal-time **E**mbedded **A**ffinity Software Engineering Research **L**ab (REAL) – that are dedicated for teaching and conducting research in the aforementioned areas. In addition, the department recently purchased new PCs to be used exclusively in courses that make the SCS tracks. Funding for hardware and software for these labs was secured through grants from the

educational program offered by Wind River Corporation, an R&D grant from Lockheed Martin Corporation, and a donation from State Farm Agency.

3. Implementation Plan

This section describes the implementation plan for achieving the goals set forth by UTEP's CS Department to increase its graduates' expertise in secure cyber-systems. The plan presents a set of objectives for each goal and, in turn, defines activities that will lead to the attainment of each objective.

Goal 1: To increase the number of qualified students who complete a Secure Cyber-Systems track at UTEP.

We define two main objectives to meet the goal of increasing the number of qualified students who enroll and successfully complete one of the Secure Cyber-Systems (SCS) tracks at UTEP. We also define the proposed activities in the subsections below to achieve the following objectives:

Objective 1a: Implement a plan to recruit students who enter the Secure Cyber-Systems tracks.

Objective 1b: Implement a plan to retain students in the Secure Cyber-Systems tracks

Objective 1a: Implement a plan to recruit students who enter the Secure Cyber-Systems tracks.

Recruitment for the SCS tracks will be carried out by the Undergraduate Program Director and the Software Engineering program Director. Involving high-school students in an Information Assurance related summer camp activity, which has been funded from the Department of Defense, is on venue for recruiting students in the undergraduate program. The department is actively seeking scholarship money to recruit students. The plan to manage scholarships is described after the Recruitment Plan.

Recruitment Plan

The Recruitment Plan incorporates several strategies. Each is described below.

Provide a web page for the SCS tracks. The departmental website needs to be improved to market the undergraduate and graduate programs sufficiently. In addition, the department will need to work with the university's scholarship office to identify sources of funding that can support students who enter one of the tracks. The website will also include stories of our graduates and where they are now, as well as announcements of any research and programs activities that highlight the success of students, such as publications, conference presentations, and student competitions. Projects material and portfolios of the graduate students in the SCS track will also be available on the website.

Recruit students from the Computing Alliance of Hispanic-Serving Intuitions (CAHSI). CAHSI [3] (http://cahsi.org) is a consortium of over 15 Hispanic-Serving Institutions from California, Texas, New Mexico, Florida, Illinois, and Puerto Rico that focuses on the recruitment, retention, and advancement of Hispanics in computing. The alliance, which is led by UTEP, promotes effective practices, including the Affinity Research Group (ARG) model and the Mentor-Grad program that focus on the development of professional, communication, and research skills, as well as the advancement of students into graduate school. The Mentor-Grad program will provide an excellent source of qualified students into our SCS tracks.

***Distribute brochures and advertise material at national conferences*.** Both the Undergraduate Program Director and the Master of Software Engineering Director have a record of presenting and attending national and international conferences in areas related to Computer Security and Software Engineering. As part of our recruitment efforts, we will develop flyers to be distributed at the relevant conferences. One of the conferences that will be of special interest is the annual Society for Advancement of Chicanos and Native Americans in Science (SACNAS) conference that attracts over 4000 attendees. CAHSI has been collaborating with SACNAS to establish a computing community at the conference. Towards this end, CAHSI has sponsored technical sessions in the area of security, among other areas, over the last three years. Both directors and the department chair will work with CAHSI to participate in the informational sessions, technical sessions, workshops, and poster presentations to promote the SCS tracks.

Recruit students from the BSCS and other programs at UTEP. A major recruiting activity will be accomplished through the Junior Professional Orientation course required for all students in the BSCS and BS in Electrical and Computer Engineering (ECE) programs. We will also define similar efforts to target eligible students in other engineering disciplines at our institution, such as Computer Information Systems, Computational Science, and Systems Engineering. We will coordinate with the faculty advisors to keep the students aware of the SCS tracks and scholarship opportunities during the academic-advising period, as well as during exit interviews, and we will coordinate with department chairs to provide us access to particular courses for brief presentations. Information about the tracks will be disseminated through fliers and brochures made available at the respective departments.

Target REU students. The CS department at UTEP, in collaboration with the departments of Psychology, Biological Sciences, Industrial Engineering, and Civil Engineering, offers an eight-week full-time NSF-funded Research Experience for Undergraduates (REU) program for qualified students in the area of applied intelligent systems. In addition, UTEP's Campus Office of Undergraduate Research Initiatives (COURI) serves as the central unit on campus for facilitating undergraduate training in research, scholarly, or creative activities, enhancing student's academic success and professional development, and showcasing the results of their work. CS faculty, who are conducting research in areas related to cyber security, will define projects to engage REU and COURI students. Eligible students from these efforts will be recruited to pursue one of the SCS tracks.

Target eligible applicants to our Master's programs. We will coordinate with the different CS graduate programs (Master's of Science in Computer Science and Master's of Science in Information Technology) to recruit eligible students into the SCS track of the MSSwE program.

Advertise through CyberWatch West website and social media. CyberWatch West (CWW) (http://www.cyberwatchwest.org/) is an NSF-funded consortium that brings together universities, public and private schools, as well as businesses and government agencies for the purpose of raising the number and quality of the national workforce in the area of cybersecurity/information assurance. UTEP became a member of CWW in October 2013. Members of the consortium collaborate to share and enhance practices, methodologies, curricula, course modules, and materials. CWW also sponsors student competitions, internships, and professional development. As part of our recruitment efforts, we

will advertise scholarship opportunities through CWW's website. Social media, such as CWW's, CAHSI's, and UTEP CS's Facebook pages will serve as another venue to disseminate opportunities.

Student Scholarship Plan

The department will actively seek funding opportunities to provide students enrolled in the SCS tracks with scholarships. All material used in advertising the scholarship program and student recruitment will have a clear description of scholarship eligibility requirements (specified below), as well contact information for the program. Once scholarship funds are secured, we will register the scholarship opportunity with UTEP's Scholarship Office. Applicants will contact the Scholarship Office directly. Applications that do not meet the eligibility criteria will be discarded, and eligible applications will be forwarded to the responsible departmental committee for recommendation. Possible requirements, application guidelines, and review process are provided next.

Scholarship requirements could be set as follows:

- GPA of 3.0 for undergraduate applicants and 3.25 for graduates.
- Junior standing in the initial semester to be funded for undergraduates
- Fulltime enrollment
- U.S. Citizenship

Applicants would be required to submit the following as part of their application:

- Signed statement of understanding of the scholarship program's requirements and commitment. This statement will be prepared by project team and included in all promotional materials.
- Official transcripts from all colleges attended.
- A personal statement describing the student's career goals in government service and cyber-security. The statement should highlight any experience in cyber-security, including courses, projects, thesis, and job experience.
- Personal résumé.
- Two recommendation letters, with at least one written by a faculty member.

Submission of applications would have a deadline of one month prior to the start of the academic year. Once the list of applicants is compiled by the Scholarship Office, their packets will be forwarded to the appropriate program director. A Selection Committee will review the applications, rank the applications individually based on the rubric presented in Table 1, discuss the rankings and make adjustments based on the discussions, and make recommendations

Objective 1b: Implement a plan to retain students in the Secure Cyber-Systems (SCS) tracks.

To ensure that students complete their respective degrees and the track, the project team will define a set of activities to develop the students' academic and social skills. We believe that students' engagement in group activities, both academic and social, enhances their successful completion of the respective program and track.

Table 1: A rubric for ranking students' applications

Category	0 Points	1 Point	2 Points	4 Points
GPA (BSCS/MSSwE)	3.0-3.1/3.24	3.2 – 3.3/3.25-3.39	3.4-3.74/3.4-3.74	3.75-4.0/3.75-4.0
Experience	No previous work experiences	Some work experiences; experiences not in CS or cyber-security	Some work experiences in CS or cyber-security (duration: one summer internship or one semester of research)	Extended work experiences in CS or cyber-security (duration: over two semesters)
Personal Statement	Statement does not address any of the following: 1)Motivation for work in cyber-security is clearly stated: 2) Motivation is tied to personal attributes/ experiences; 3) presents solid long-term goals; 4) provides concrete examples of his/her areas of cyber-security areas of interests; 5) describes broader impact of scholarship.	Statement addresses at most 2 out of the following: 1)Motivation for work in cyber-security is clearly stated: 2) Motivation is tied to personal attributes/ experiences; 3) presents solid long-term goals; 4) provides concrete examples of his/her areas of cyber-security areas of interests; 5) describes broader impact of scholarship.	Statements addresses at most 3 out of the following: 1)Motivation for work in cyber-security is clearly stated: 2) Motivation is tied to personal attributes/ experiences; 3) presents solid long-term goals; 4) provides concrete examples of his/her areas of cyber-security areas of interests; 5) describes broader impact of scholarship.	Statements addresses at least 4 out of the following: 1)Motivation for work in cyber-security is clearly stated: 2) Motivation is tied to personal attributes/ experiences 3) presents solid long-term goals; 4) provides concrete examples of his/her areas of cyber-security areas of interests; 5) describes broader impact of scholarship.
Recommendation Letters	Both letters do not describe personal attributes of applicant	Only one letter describes personal attributes, but does not provide evidence of student's potential for success.	Both letters describe personal attributes, but only one provides evidence of student's potential for success.	Both letters describe personal attributes and provide evidence of student's potential for success.

Student Development and Retention Plan

Create a Cyber-Security Affinity Group. The Affinity Research Group (ARG) Model [4] enhances students' abilities to learn, use, and integrate the necessary knowledge and skills needed for research with those essential for effective team work. Although the ARG model was initially created as a vehicle to ensure involvement and success of undergraduate students in research, the model has been shown to be effective in creating communities of practice that prepares students for success in professional careers.

Although students seeking one of the SCS tracks and funded by scholarships may belong to different research groups within the CS department, work on different projects, and participate in different classes, we will hold monthly group meeting or workshops for the students on scholarships with the goal of achieving the following:

- Sharing of knowledge and experiences among the members of the group
- Enhancing the group members' soft skills such as communication both oral and written and team skills
- Allowing participants to seek the advice and help from each other as well as faculty members
- Establishing a community of students that gives group members a sense of belonging.

A major component of the ARG model calls for the celebration of individual and team achievements. During the recurring group meetings, the project faculty members will highlight and celebrate individual students' achievements in the different projects, classes, and competitions in which they participate.

Involve students in cyber-security competitions. Students who receive funding will be asked to participate in local and national student competitions. This participation can be at an individual or team level. While the focus will be on competitions related to cyber-security, the students will also be encouraged to participate in different competitions in the computer science and software engineering areas. The directors will announce applicable competitions to students and will work with the students to form teams (if applicable) and prepare for such competitions.

Goal 2: To graduate students who can enter the workforce with the ability to transfer state-of-the-art cyber-security techniques and approaches into practice.

We define two main objectives to meet the goal of graduating students with the ability to transfer state-of-the-art cyber-security techniques and approaches into practice. We also define the proposed activities to achieve these objectives:

Objective 2a: To implement a continuous quality improvement plan to ensure that funded students are prepared to contribute to the cyber-security workforce.

Objective 2b: Engage students in projects related to cyber-security.

Objective 2a: Implement a continuous quality improvement plan to ensure that the SCS curricula prepare students to enter the cyber-security workforce.

UTEP has defined SCS tracks within the Bachelor of Science in Computer Science (BSCS) and the Master's of Science in Software Engineering (MSSwE) programs. In order to achieve Objective 2a we plan on providing students with appropriate learning experiences through the courses in these tracks.

Initial Work

BSCS-SCS Curriculum. The BSCS program has been accredited by ABET's Computer Science Accreditation Board since 1986. It provides a strong base in problem solving skills, programming skills, knowledge of computer architecture, computer science theory, and practical experience in applying the computer to the solution of problems. The department follows a Continuous Quality Improvement process to

maintain the relevance of the degree plan. The BSCS degree plan now requires 120 credit hours of course work including 49 credit hours of Computer Science courses, 19 credit hours of Mathematics courses, 12 credit hours of Science courses, 4 credit hours of Digital Systems Design, and 36 hours of core courses. The 49 credit hours of Computer Science courses include 15 credit hours of technical electives and 6 credit hours of a capstone project based Software Engineering courses.

The Secure Cyber-Systems (SCS) Track within the BSCS program requires students to take a set of courses with significant computer security contents for their technical electives. The set of course outcomes in the BSCS degree with the SCS track was designed to cover all the required Knowledge Units and an adequate number of optional Knowledge Units associated with the NSA Center of Academic Excellence Cyber Operations designation. In addition to being exposed to computer security related concepts in courses required in the BSCS degree plan (Computer Architecture, Operating Systems, Software Engineering, Automata), students in the SCS track are required to take 4 computer security related courses as indicated in Table 2.

Table 2: Course Selection for the BSCS-SCS Track

Prefix and Number	Courses	SCH
	Required Courses	
CS 4316	Computer Networks	3
CS 4351	Computer Security	3
CS 4387	Software Integration and V&V	3
	One of the following electives	
CS 3320	Computer Architecture II	3
CS 4317	Human-Computer Interaction	3
CS 4330	Mobile Application Development	3
CS 4376	Computational Decision-Making/Risk Analysis for Security	3
CS 4377	Cyber-Security for Critical Operational Technology	3
Total credit hours for the SCS track		12

MSSwE-SCS Curriculum. The MSSwE program is based on the Software Engineering Body of Knowledge (SWEBOK) [5], the Certified Software Development Professional (CSDP) program [6], the Institute of Electrical and Electronics Engineers- Computer Society (IEEE-CS) and the Association for Computing Machinery (ACM) Graduate Software Engineering 2009 (GSwE2009) curriculum [7]. The MSSwE program consists of three parts. In the first part, students take courses that prepare them to take the Certified Software Development Professional (CSDP) certification examination. The CSDP program is sponsored by the IEEE-CS, one of the world's leading organization of computing professionals. In the second part of the MSSwE program, students acquire depth and breadth to software engineering knowledge areas and domains with a special focus on the development of secure, safety-critical, real-time embedded

systems. While students work on small team projects throughout much of their program of study, the third part of the program focuses on providing students with practical project experience by working within a team to develop a software component of an overall physical system. Both individual courses projects as well as projects used in the final practicum course will have applications in the security and reliability of an embedded software system. In addition, students in the program are encouraged to seek internships and work on industry projects while they are in the program. Students are allowed to substitute applicable internship experience for three credit hours in the program.

The Secure Cyber Systems (SCS) Track within the MSSwE program is designed to produce graduates capable of building software systems or components that are robust and secure enough to ensure correct and secure functionality of a complex cyber-physical system. The MSSwE-SCS track is based on the Software Engineering Institute's Master of Software Assurance Reference Curriculum (MSwA) [8]. MSwA was developed based on the needs of entities such as DHS and the National Cyber Security Division (NSCD), a division of the Office of Cyber Security & Communications. Although the curriculum recommendations encompass a wide range of topics related to software assurance in general, there is a special emphasis on software security as noted by the following definition of software assurance [8]:

> Application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures.

Table 3: Required Courses in the MSSwE program

Prefix and Number	Required Courses	SCH
CS 5374	Software Construction	3
CS 5385	Software Requirements Engineering	3
CS 5386	Software Architecture & Design	3
CS 5387	Software Integration and V&V	3
CS 5388	Software Project Management	3
CS 5389	Software Engineering Practicum	3
Total credits from core courses		18

The curriculum for the MSSwE-SCS track consists of three parts. In the first part, students take five core courses that enhance their knowledge of the central ideas, methods, and techniques associated with software engineering. The list of five courses required for the track is the same as that of the general MSSwE program. In the second part, students acquire depth and breadth to the area of secure software engineering. In this part, students take four additional courses that will enhance their abilities to develop reliable and secure cyber-physical systems. The program's courses will engage students in hands-on projects to strengthen their ability to learn and apply state-of-the-art practices in software development.

Both the general MSSwE program and the SCS track require students to complete 30 semester credit hours. Of these, 18 semester credit hours are required courses (refer to Table 3). Students pursuing the MSSwE-SCS track are also required to take CS 5352 (Computer Security), as well as, three other courses from the list of prescribed electives shown in Table 4.

Table 4: Course Selection for the MSSwE-SCS Track

Prefix and Number	Prescribed Elective Courses	SCH
CS 5316	Computer Networks	3
CS 5352*	Computer Security	3
CS 5371	Software Safety and Risk Analysis	3
CS 5372	Specification and Design of Real-Time Systems	3
CS 5375	System Security Assurance	3
CS 5376	Computational Decision-Making and Risk Analysis for Security	3
CS 5377	Cyber-Security for Critical Operational Technology	3
Each student in the program is required to take four elective courses.		12
*Computer Security is a required course for the MSSwE-SCS track		

The following is the catalog description of the most relevant courses in the BSCS SCS track (4xxx course numbers) and in the MSSwE-SCS track (5xxx course numbers).

CS 4316/5316: Computer Networks. Introduction to data communications. Covered topics include: data transmission, link control, encoding, multiplexing, switching, network topologies, address resolution, protocol layering, routing methods, data security, and distributed systems. The graduate course extends the course to include advanced topics, e.g., computer network architecture and programming.

CS 4351/5352: Computer Security. General concepts and applied methods of computer security, especially as they relate to confidentiality, integrity, and availability of information assets. Topics include system security analysis, access control and various security models, identification and authentication, protection against external and internal threats, communication protocols and internet security.

CS 5371: Safety and Risk Analysis. Principles of software development for safety and mission critical systems. Topics include safety-related analysis, specification, design, implementation, and maintenance techniques; survey of programming language and operating system issues for implementing safety-related software; safety requirements, hazard and risk analyses, fault tolerance, basics of software reliability, and issues of verification, validation, and certification; models for safety in a distributed system; safety standards and guidelines across application domain and selected tools supporting safety assurance of software components

CS 5372: Specification and Design of Real-Time Systems. Basic concepts, methods, and techniques used in the specification, design, implementation, and testing of real- time embedded software components. Topics include the characteristics of real-time systems, differences between real-time operating systems

and general operating systems capabilities, schedulability analyses, degraded mode analyses, software design patterns for real-time systems, methods specifically suited for real- time systems and verification and validation of real-time embedded systems.

CS 5375: System Security Assurance. The course focuses on incorporating security technologies and methods into new and existing systems; learning how attackers expose vulnerabilities; analyzing threats; applying methods to prevent and defeat attacks; and understanding the ethical responsibilities and obligations associated with developing, acquiring, and operating software systems.

CS 4376/5376: Computational Decision-Making and Risk Analysis for Security. The course covers a variety of mathematical and computational techniques for modeling and analyzing security problems; fundamentals of mathematical approaches for analyzing risk, decision-making under uncertainty, adversarial reasoning, extracting patterns from data for modeling and analysis; and methods to analyze security problems in rigorous ways. The course includes case studies and examples related to security to illustrate techniques and contemporary issues in cyber-security.

CS 4377/5377: Cyber-Security for Critical Operational Technology. The course explores a variety of topics associated with the cyber-security of operational technology supporting critical sectors as defined by the U.S Department of Homeland Security. The course provides hands-on experience on the construction and configuration of cyber-infrastructures to secure critical operational technology components such as Programmable Logic Controllers (PLC). Students work in teams to simulate an operational technology component using off-the-shelf hardware and software, and develop a secure cyber-infrastructure to prevent the component from being compromised.

CS 4387/5387: Software Integration and V&V. The course covers the principles and processes of validation, verification, and integration within a disciplined software development environment. Topics include efficient integration of software systems or components that meet customer requirements and needs; disciplined approaches for integration and testing throughout the development life cycle, selection of alternative methods for integration and testing, and fault diagnosis; use of static and dynamic testing techniques and tools to identify code vulnerabilities; testing based on attack patterns; and penetration testing.

Cyber-Security CQI Process

The Secure Cyber-Systems Continuous Quality Improvement (CQI) process will be adopted from the CQI process defined by the BSCS program for ABET (Accreditation Board for Engineering and Technology) accreditation. The current CQI process consists of four main CQI subcommittees that review course outcomes and ensure that the learning outcomes are being met: Fundamentals, Languages, Software, and Systems. We will define a specialized CQI subcommittee, called Secure Cyber-Systems, which will be charged with the assessment of the graduate and undergraduate SCS tracks. The undergraduate track will be assessed in the spring semester of even years and the graduate track will be assessed in the spring semester of odd years. It is important to note that the CS department has recently applied and is currently under review for the designation by the National Security Agency as a Center of Academic Excellence in Cyber-Operations. Part of achieving and maintaining this designation is the definition and implantation of CQI and Assessment plans for the SCS tracks.

The following assessment instruments will be used to evaluate the SCS tracks: Graduating Senior Survey, Alumni Survey, Employer's Survey, Senior Exit Interviews, Course Assessments, Advisory Board, and industry feedback. In order to ensure that our graduates meet specific workforce needs, the directors will engage scholarship and internships sponsors to ensure that the curriculum is preparing students to meet workforce needs. The Secure Cyber-Systems CQI subcommittee chair will ensure that the instructors assess the courses associated with their area during the scheduled semester or year. The subcommittee members will write the Continuous Quality Improvement (CQI) report in conjunction with the Chair of the Department, and they will lead a discussion at a faculty meeting regarding the results of the report and recommendations. The *charge of the subcommittee members* is to map assessment instruments to course outcomes, determine whether the program meets the learning outcomes and needs of the constituencies, and document the results and observations about the courses. The instructors will provide course material to include examples of graded exams, laboratory assignments, and other pertinent material.

Objective 2b: Engage students in projects related to cyber-security

Identification of Projects

The aim of the SCS tracks offered by the CS department is to enhance students' ability to apply state-of-the-art techniques and methodologies of software security, reliability, and safety to real-world problems. To enable students to gain hands-on experiences in the classroom, each of the elective courses that make up the SCS tracks is designed to have a semester-long team project with a focus on cyber-security. These projects will include one or more of the following elements:

- Design and implement secure software components
- Verification of software components against security and reliability quality attributes
- Management of risk within software systems
- Identification of vulnerabilities within software design and code

In order to identify appropriate projects for these courses we have defined multiple approaches:

Work with Scholarship/Internship sponsors. In order to ensure that our graduates meet specific workforce needs, the directors will engage sponsors in identification of projects that will prepare students to enter a particular segment of the workforce. For example, we are currently working with Lockheed Martin to identify a project related to security of real-time embedded systems to be used in the CS 5389 (Software Engineering Practicum) course in fall 2014.

Involve key constituencies. We will work with members of the Computer Science Advisory Board and other key constituencies to identify projects that develop essential skills and knowledge needed to prepare our students to become productive members of the workforce.

Incorporate faculty members' experiences. All faculty members teaching courses in the SCS tracks have research interests in cyber-security. The adjunct faculty members who teach SCS courses hold positions in the SCS areas, e.g., Advanced Systems Manager in UTEP's Regional Cyber & Energy Security Center and Computer Scientist at the Army Research Lab at White Sands Missile Range, Ethical Hacking group.

It is a common practice by our faculty to define class projects based on their research and industrial experiences.

Collaborate with members of CWW to identify projects. Some of the advantages provided for members of CWW include:

- Assistance with curriculum development: Help member institutions implement or adapt CyberWatch West's model curriculum, certificates and degrees in Cybersecurity/IA.
- Assistance in mapping of courseware to the Committee on National Security Systems (CNSS) standards.
- Faculty development through sponsored training and the Graduate Faculty Program.

We plan to collaborate with members of CWW to share ideas in identifying course projects and the implementations of these projects. We also aim to define collaborative projects that can be implemented across member institutions. The Undergraduate Program Director serves as UTEP's point of contact to CWW.

Integration of Projects in Coursework

Once appropriate projects have been identified for the SCS tracks' courses, these projects will become a major component of courses in the tracks. Each course will have a semester-long team project where students work in teams to fulfill elective requirements as part of the BCSC and MSSwE programs. The Undergraduate Program Director will lead the undergraduate SCS track within the CS department and the MSSwE Program Director will ensure that courses related to the SCS MSSwE track include an appropriate semester project component.

Goal 3: To place students in government positions that utilize their knowledge and capabilities in cybersecurity.

We define two main objectives to meet the goal of placing students in positions that utilize their knowledge and capabilities in cybersecurity. We also define the proposed activities to achieve these objectives:

Objective 3a: Involve UTEP's Career Services to promote UTEP's expertise in cybersecurity.

Objective 3b: Establish strong communications with industry and government.

Objective 3a: Involve UTEP's Career Services in promoting UTEP's expertise in cybersecurity.

UTEP has an established Career Service Center that works with both students and potential employers to identify and advertise opportunities for student employment. The Center will also connect us with potential employers who register openings that match SCS expertise. Activities established by the career service center that help connect employers to students include:

- Career Fairs – one held in the fall semester and another in the spring semester
- Internship and Part-time Job Fairs – one held in the fall semester and another in the spring semester
- Graduate and Professional School Fair

- Connections – Engineering and Science Job Expo

Internship and job placement

We will collaborate with the UTEP Career Center to identify internships and job opportunities related to cyber-security and software assurance. Once internship or fulltime opportunities become available, we will advertise SCS opportunities on the CS departmental website, and we will encourage students to pursue these opportunities during our group meetings.

Objective 3b: Establish strong communications with industry and government.

There are two main mechanisms by which we will build strong communications with industry and government. One is through the internships that our students acquire and the other is through involvement of high-level managers in the department's Board of Advisors. Each is discussed next.

Internships. In an effort by the College of Engineering and the CS department at UTEP to ensure that students in our programs gain practical experiences beyond those offered in class projects, we have recently (summer 2013) changed the curriculum to allow students to receive credit for internship experiences. In the CS department, we have defined a process to ensure the applicability of the internship experience to student's field of study. This process is also in place to ensure that our students contribute quality work at the internship offering entity. The established internship-for-credit process includes a description of students' expected activities as part of the internship. This must be completed by a potential internship supervisor employer. This description must be approved by an academic advisor as part of the agreement between the student and the CS department for the internship-for-credit approval. Once the student is involved in the internship, he or she is required to provide a mid-internship status report to show alignment of work with the previously stated agreement. At the end of the internship, the student's supervisor is required to complete a form that includes evaluation of the student's performance and future recommendations.

The aforementioned process is an important activity to help us establish contact with industrial and government entities, as well as to ensure that our students do indeed deliver quality work. This is essential to ensure hiring of future student interns and graduates.

***Involvement via the Advisory Board*.** The CS department has a strong and diverse Advisory Board that includes representatives from government, government contractors, academia, and industry. Many of the members have interest in cyber-security and software assurance. In particular, Lockheed Martin Corporation (LMC) and the Office of Naval Research (ONR) have worked with the department to incorporate cyber-security into the curricula and research activities; in particular, they have participated in the definition and critical review of the SCS tracks, discussed with the faculty potential research projects, and assisted in the real-time systems laboratory setup. Both LMC and ONR have indicated strong interest in establishing a pipeline for hiring our graduates that starts with summer internships and leads to fulltime employment.

References

[1] U.S. Department of Defense "Strategy for Operating in Cyberspace," July, 2011, [Accessed Mar. 25, 2014]. Available from: http://www.defense.gov/news/d20110714cyber.pdf

[2] White House "National Security Strategy", May, 2010, [Accessed Mar. 25, 2014]. Available from: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[3] Gates, A. Q., Hug, S., Thirty, H., Aló, R., Beheshti, M., Fernandez, J., Rodriguez, N. & Adjouadi, M. "The Computing Alliance of Hispanic-Serving Institutions: Supporting Hispanics at Critical Transition Points," *ACM Transactions on Computing Education, BPC Special Edition*, 11(6), October 2011.

[4] Villa, E., Gates, A., Kephart, K., Hug, S., and H. Thirty, "Affinity Research Groups in Practice: Apprenticing Students in Research," *Journal of Engineering Education,* July 2013, 102(3), pp. 444-466. DOI 10.1002/jee.20016

[5] SWEBOK, Guide to the Software Engineering Body of Knowledge, P. Bourque and R. Dupuis (Eds.). IEEE Computer Society Press, 2004. [Accessed Mar. 25, 2014], Available from: http://www.computer.org/portal/web/swebok

[6] IEEE Computer Society, *Certified Software Engineering Professional* web site, 2001, [Accessed Mar. 25, 2014]. Available from: http://computer.org/certification

[7] Pyster, A. (ed.), Graduate Software Engineering 2009 (GSwE2009) Curriculum Guidelines for Graduate Degree Programs in Software Engineering, Integrated Software & Systems Engineering Curriculum Project, Stevens Institute, September 30, 2009, [Accessed Mar. 25, 2014]. Available from: http://www.gswe2009.org/curriculum/recommendations/document/

[8] Mead, Nancy R., Allen, Julia H., Ardis, Mark, Hilburn, Thomas B., Kornecki, Andrew., Linger, Richard., and McDonald, James., "*Software Assurance Curriculum Project, Volume I: Master of Software Assurance Reference Curriculum"* (CMU/SEI-2010-TR-005). Software Engineering Institute, Carnegie Mellon University, 2010, [Accessed Mar. 25, 2014]. Available from: http://www.sei.cmu.edu/library/abstracts/reports/10tr005.cfm