ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #36657

Development of a Joint Cybersecurity Graduate Program at Mercer University

Dr. Donald U Ekong P.E., Mercer University

Dr. Ekong is the Program Director for Computer Engineering, Cybersecurity, and Software Engineering at Mercer University's School of Engineering. He received his B.Eng. in Electrical Engineering at the University of Port Harcourt, and his M.Sc. and Ph.D. in Electrical Engineering at the University of Saskatchewan. He is also licensed professional engineer in the state of Georgia, a Senior Member of IEEE, and a registered engineer in the province of Saskatchewan, Canada. Before coming to Mercer University in 2002, he worked in industry as a Senior Software Engineer at Ciena Corp in Alpharetta, GA, Senior Software Engineer at Motorola in Tempe, AZ, and a Systems Engineer at Valmet Automation, Calgary, Canada. His teaching and research interests include using mobile technologies to improve healthcare in under-served and low-resource communities, cybersecurity including software security, computer networks, and microcontrollers/embedded systems.

Dr. Stephen Hill, Mercer University

Stephen Hill earned his BS in General Sciences from Morehouse College and his BSME, MSME, and Ph.D. from the Georgia Institute of Technology. He is currently an associate dean and associate professor in the School of Engineering at Mercer University. He worked for the oilfield services giant Schlumberger for 14 years before.

Development of a Joint Cybersecurity Graduate Program at Mercer University

Donald U. Ekong and Stephen Hill
School of Engineering, Mercer University

Abstract

This paper discusses the development of a new MS in Cybersecurity program at Mercer University. This is a joint program between the School of Engineering, the Computer Science program (in the College of Liberal Arts and Sciences), and the School of Business. This program requires 30 credit hours, and it has three different tracks. The program also includes 12 credit hours of common core. This paper discusses how the program will be assessed, and how the program aligns with the NICE framework.

Keywords

Cybersecurity education, curriculum, assessment

Introduction

During the 2020-21 academic year, the Board of Trustees at Mercer University approved a new Master of Science in Cybersecurity program. This was in response to the growing demand, nationwide and locally, for cybersecurity professionals[1], as well as the need of graduates from various backgrounds who wish to either enter the cybersecurity field, or get more training in cybersecurity. The program is a joint program between the School of Engineering, (the undergraduate cybersecurity program in) the College of Liberal Arts and Sciences, and the School of Business. The degree is awarded by the School of Engineering, and requires 30 credit hours of graduate course work. The program was first published in the university's academic catalog during the 2021-22 academic year. The first iteration of this joint program had four core areas: Cybersecurity for Business, Cybersecurity Operations, Embedded Computer Systems/IoT with Cybersecurity, and Software Security. The program required three foundation courses (9 hours), four courses from a core area (12 hours) and three elective courses, including thesis or other approved courses (9 hours). Accorning to the initial plan, the Business school would be in charge of the Cybersecurity for Business core area; the College of Liberal Arts and Science (which housed the undergraduate Cybersecurity program) whould be in charge of the Cybersecurity Operations core area; and the School of Engineering would be in charge of the Embedded Computer Systems/IoT with Cybersecurity, and Software Security core areas.

During the 2021/22 academic year, representatives of the participating schools met again to take another look at the joint program and assign responsibility for the courses that would be taught. The representatives agreed to redesign the program, and reduce the number of core areas to three tracks based on the availability of faculty. The consolidated tracks include: Cybersecurity for Business track (Business school), Cyber-physical and Secure Software Systems track (College of Liberal Arts and Sciences, and the Engineering school), and General track. The foundation courses (which is similar for each track) was increased to four courses (12 hours). The other

courses for each track will be described in the next section. The business track is primarily for students with an undergraduate degree in Business. The Cyber-physical and Secure Software Systems track is primarily for students with an undergraduate degree any of the following areas: Computer Science, Cybersecurity, Engineering, and Information Technology. The General track is primarily for students from all backgrounds.

Curriculum

The Master of Science in Cybersecurity program requires thirty credit hours of graduate work. Graduate courses in the School of Engineering are courses at 500 and 600 levels. 500-level courses may be co-located with senior-level (4xx) undergraduate courses, with extra work done by graduate students in those courses. A minimum of eighteen of the thirty credit hours must be completed in the Cybersecurity discipline. Out of these eighteen credit hours in the discipline, a minimum of twelve credit hours must be at the 600 level. The program also requires that a minimum of eighteen of the thirty credit hours must be completed at the 600 level. The program has a thesis option which requires six credit hours of research.

The program has three tracks, namely Cybersecurity for Business track, Cyber-physical and Secure Software Systems track, and General track. Each track has four foundation courses (12 hours). The foundation courses are the same for all the tracks. The Business track and the Cyber-physical and Secure Software Systems track, each have two core courses (6 hours), and four elective courses (12 hours). The General track has six elective courses (18 hours). Table 1 lists the foundation courses, Table 2 lists the Business track core courses, and Table 3 lists the core courses in the Cyber-physical and Secure Software Systems track.

Table 1. Foundation Courses

CYS 601	Information Security and Assurance
CYS 602	IT Principles and Applications
CYS 523	Cybersecurity Law, Ethics, and Policy
CYS 621	Cybersecurity Governance and Risk Management

Table 2. Cybersecurity for Business Track’s Core Courses

CYS 603	Cybersecurity Experimentation
CYS 653	Business and IT Service Strategy

Table 3. Cyber-physical and Secure Software Systems Track's Core Courses

CYS 603	Cybersecurity Experimentation
CYS 574	Secure Hardware and Cyber-physical Systems

The elective classes are other graduate Cybersecurity courses, as well as approved graduate courses in business and engineering. Table 4 shows the overall MS in Cybersecurity curriculum's class distribution.

Table 4. Class Distribution

Fall Semester	**Spring Semester**
CYS 601 Information Security and Assurance	CYS 523 Cybersecurity Law, Ethics, and Policy
CYS 602 IT Principles and Applications	CYS 621 Cybersecurity Governance and Risk Management
CYS 5xx/6xx CYS Course	CYS 603 Cybersecurity Experimentation
XXX 5xx/6xx Graduate Course	XXX 5xx/6xx Graduate Course
XXX 6xx Graduate Course	XXX 6xx Graduate Course

The XXX courses are graduate cybersecurity courses and approved graduate courses in business and engineering.

Assessment Plan

Graduate programs at the Mercer University's School of Engineering are assessed by the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC). This agency is responsible for accrediting degree-granting higher education institutions in the Southern states of USA. The initial assessment of the program will be performed on one of the foundational courses, CYS 601. The assessment consists of two parts one being an assessment by faculty and the other allowing the students to self-assess their development. For the both assessments, the Student Learning Outcomes presented in Table 5 are assessed.. .

Table 5. Student Learning Outcomes (SLO)

SLO	Description
1	Students demonstrates appropriate depth in cybersecurity in solving complex problems.
2	Students will demonstrate the capability to communicate technical aspects of the solution for cybersecurity problems to a technical audience.

The faculty assessment requires three faculty who teach in the area to assess an artifact that can be either a complex assignment, project, or exam. Each faculty would rate each student based on the following established rubric that is currently being used for the other graduate courses in the engineering program:

- 5- Fully understands the problem and solution is complete and explanations are clear. Solution consists of a series of logical and easy to interpret steps that progress from the initial statement to a final answer. Able to communicate all details of the problem.
- 4- Understands the problem and solution is complete but there are a few minor errors. Solution consists of a series of logical steps that progress from the initial statement to a final answer; however, few details are missing in communicating the technical aspect of the solution.
- 3- Understands the problem, but there are a few logical flaws in the solution. Solution is not presented clearly in a series of steps that progress from the initial statement to a final answer. Some details are missing, which makes it difficult to fully communicate the solution.
- 2- There is a lack of understanding of the problem and the solution is incomplete with some serious logical flaws. Solution is not presented in a series of steps that progress from the initial statement to a final answer, which makes it very difficult to communicate the technical aspects of the solution.
- 1-No understanding of the problem. No solution is presented or the solution is completely wrong. There is no or poor communication of technical aspects of the solution.

Mapping to NICE Framework

The Workforce Framework for Cybersecurity, also known as the NICE Framework, provides a common definition of cybersecurity, a comprehensive list of cybersecurity tasks, and the knowledge, skills, and abilities required to perform those tasks[2]. It was first created after 20 governmental departments and agencies, representatives from the private sector, and academia came together to determine how to provide a common understanding of cybersecurity work[3]. The

initial framework has undergone some revisions since it was first created in 2017. One of the main goals of the NICE Framework is to help the US market fill its need for cybersecurity professionals and provide a common language with which organizations, job recruiters and education institutes can communicate[4].

The NICE Framework is comprised of the following components[2]:

- Categories (7) – A high-level grouping of common cybersecurity functions.
- Specialty Areas (33) – Distinct areas of cybersecurity work.
- Work Roles (52) – The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role.

The seven categories include[2,4]: Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Operate and Collect, and Investigate.

CYS 601 (Information Security and Assurance), a foundation course, and CYS 603 (Cybersecurity Experimentation), a core couse, map into the following NICE Framework categories: Securely Provision, Operate and Maintain, and Protect and Defend. Two other foundation courses - CYS 621 (Cybersecurity Governance and Risk Management) and CYS 523 (Cybersecurity Law, Ethics, and Policy) map into the Oversee and Govern category. The fourth foundation course, CYS 602 (IT Principles and Applications), maps into the Operate and Maintain category.

Summary and Conclusions

A new MS in Cybersecurity program has been started at Mercer University. This program requires 30 credit hours, and is a joint program between the School of Engineering, the Computer Science program (in the College of Liberal Arts and Sciences), and the School of Business. The first set of students started in the 2022-23 session. The program has three different tracks, and it is open to students with technical and nontechnical backgrounds. All track areas can also prepare students for a broad cybersecurity certification.

References

1 U.S. Bureau of Labor Stattistics. (2022). Retrieved from: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

2 Workforce Framework for Cybersecurity (NICE Framework). (2022). Retrieved from: https://niccs.cisa.gov/workforce-development/nice-framework

3 NIST Special Publication 800-181, rev.1. (2017) Workforce Framework for Cybersecurity (NICE Framework).

4 Alsmadi, I. (2018). Cybersecurity Education Based on the NICE Framework: Issues and Challenges. *ISACA Journal, Vol 4*. Retrieved from: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/cybersecurity-education-based-on-the-nice-framework-issues-and-challenges

Donald U. Ekong

Dr. Ekong is the Program Director for Computer Engineering, Cybersecurity, and Software Engineering at Mercer University's School of Engineering. He received his B.Eng. in Electrical Engineering at the University of Port Harcourt, and his M.Sc. and Ph.D. in Electrical Engineering at the University of Saskatchewan. He is also licensed professional engineer in the state of Georgia, a Senior Member of IEEE, and a registered engineer in the province of Saskatchewan, Canada. Before coming to Mercer University in 2002, he worked in industry as a Senior Software Engineer at Ciena Corp in Alpharetta, GA, Senior Software Engineer at Motorola in Tempe, AZ, and a Systems Engineer at Valmet Automation, Calgary, Canada. His teaching and research interests include using mobile technologies to improve healthcare in under-served and low-resource communities, cybersecurity including software security, computer networks, and microcontrollers/embedded systems.

Stephen Hill

Stephen Hill earned his BS in General Sciences from Morehouse College and his BSME, MSME, and Ph.D. from the Georgia Institute of Technology. He is currently an associate dean and associate professor in the School of Engineering at Mercer University. He worked for the oilfield services giant Schlumberger for 14 years before.