Earn your Master of Cybersecurity Engineering degree from one of only sixteen universities in the nation designated by the National Security Agency and the Department of Homeland Security as a "Center of Academic Excellence in Cyber Defense Education, Center of Academic Excellence in Cyber Defense Research and Center of Academic Excellence in Cyber Operations."

AUBURN

ENGINEERING

Department of Computer Science and Software Engineering
3101 Shelby Center
Auburn, AL 36849

Xiao Qin
Graduate Program Officer
Phone: 334.844.6327
Fax: 334.844.6329
Email: xqin@auburn.edu

Master of Cybersecurity Engineering

Program Overview

Auburn University's cybersecurity engineering graduate program prepares students for analyzing, developing, investigating, protecting, and defending the cyber ecosystem of organizations. As such, it focuses on the engineering and technical aspects of cybersecurity. The degree is designed to appeal to practioners as well as research scholars through the choice of capstone experience.

The Master of Cybersecurity Engineering equips students with the advanced education required to analyze, develop, investigate, protect and defend computer information systems.

This degree program focuses on the engineering and technical aspects of cybersecurity.

The Cybersecurity Engineering graduate degree can be earned entirely through on campus instruction, through the Engineering graduate online program, or a combination of the two. Distance students should note that MATH 6180, Cryptography, is offered only in an on campus format and cannot include it as one of their elective cybersecurity specific courses.

Program Outcomes

Outcome 1: Understanding of computer science principles beyond the baccalaureate level. This is assessed by successful completion of foundational courses.

Outcome 2: Acquisition of skills specific to identifying and assessing cybersecurity threats, developing suitably protective and resilient network and software mechanisms, defending against cyber attacks, and detecting, triaging and mitigating cybersecurity breaches. This is assessed by successful completion of cybersecurity specific courses.

Outcome 3: Acquisition of skills relevant to the workforce. This is assessed by successful completion of a capstone project.

Admission Requirements

Applicants should have a baccalaureate degree in computer science, software engineering or an equivalent technically deep software-oriented equivalent discipline from an institution of recognized standing. Degrees or significant work experience in information technology, electrical engineering or other related disciplines may also be suitable. Applications will be evaluated on an individual basis by the department's graduate admission committee.

Program Requirements

The Master of Cybersecurity Engineering degree entails a minimum of 33 semester graduate credit hours. The following courses are required:

Foundational Courses: 9 Credit Hours

- COMP7270/7276 Advanced Algorithms
- COMP7300/7306 Advanced Computer Architecture
- COMP7500/7506 Advanced Operating Systems

Required Cybersecurity Courses: 9 Credit Hours

- COMP6350/6356 Digital Forensics
- COMP6370/6376 Computer and Network Security
- COMP7370/7376 Advanced Computer and Network Security

Elective Cybersecurity Courses: 9 Credit Hours

- MATH6180 Cryptography
- COMP6520/6526 Network and Operating System Administration
- COMP6700/6706 Software Process
- COMP6720/6726 Real Time and Embedded Systems
- COMP7700/7706 Software Architecture
- COMP7710/7716 Software Environments
- COMP7720/7726 Software Re-Engineering

Elective Courses: 3 Credit Hours

- 6000/7000/8000 level coursework relevant to cybersecurity and approved by the major professor.

Capstone Experience: 3 Credit Hours

- COMP7980/7976 Capstone Engineering Project

A capstone engineering project demonstrating mastery of cybersecurity engineering is required for the degree. The project includes both software and a written report.