Master of Science in Cybersecurity Engineering (MS-CYBE)

Prepare for a secure future

The MS-CYBE 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 practitioners as well as research scholars through the requirement of capstone experience.

Students who complete the MS-CYBE degree also receive the National Centers of Academic Excellence in Cybersecurity in Cyber Defense (CAE-CD) designation.

Curriculum

The MS-CYBE degree entails a minimum of 33 semester graduate credit hours:

- **Foundational Courses**: 3 Credit Hours
  - COMP7500 Advanced Operating Systems*

- **Required Cybersecurity Courses**: 18 Credit Hours
  - COMP6530 Secure Cloud Computing
  - COMP6350 Digital Forensics*
  - COMP6370 Computer and Network Security*
  - COMP6830 Cybersecurity Threats and Countermeasures*
  - COMP7720 Software Reverse Engineering
  - COMP7370 Advanced Computer and Network Security*

- **Elective Cybersecurity Courses**: 9 Credit Hours
  - COMP6000/7000/8000-level coursework relevant to cybersecurity.

- **Capstone Experience**: 3 Credit Hours
  - COMP7980 Capstone Engineering Project*

Requirements

MS-CYBE candidates are expected to 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.

Learning Outcomes

- **CDE 1**: Students have an understanding of fundamental concepts of cybersecurity.
- **CDE 2**: Students know prevalent cybersecurity threats, threat models (such as Man-in-the-Middle), and canonical defenses.
- **CDE 3**: Students have the ability to identify, assess, and defend against cybersecurity threats; develop defendable and resilient network and software mechanisms; and detect and investigate cybersecurity breaches.
- **CDE 4**: Students are versed in techniques for gathering and preserving digital forensic evidence relating to a cyber event.
- **CDE 5**: Students possess a knowledge of computer science (e.g. algorithms, operating systems, computer architectures, ethics, etc.), and have the ability to leverage this knowledge for a deeper contextualized understanding of cybersecurity.
- **CDE 6**: Students communicate cybersecurity issues effectively.
- **CDE 7**: Students have the ability to apply their cybersecurity capabilities in an integrated manner to address specific cybersecurity problems.

* Courses that satisfy the National Centers of Academic Excellence in Cybersecurity requirements for Cyber Defense (CAE-CD).