CYBER SECURITY, MASTER OF SCIENCE

Overview

Overview

The master program in cyber security aims to prepare graduates for the highly demanding market of cyber security and related fields. We aim to integrate knowledge and skills from cyber security with data science and software engineering and leverage those different disciplines in our department. The curriculum for the master program in cyber security is interdisciplinary in nature within areas relating to cyber security, such as data analytics, software engineering, and computer forensics. This curriculum will draw on various courses that will be used to provide context for the traditionally required methodological, quantitative, and theoretical courses. The program will meet the high demands for cyber security at the state and national levels.

Admissions

Admission Requirements

A student must be admitted to Graduate Studies and to a specific program in order to take graduate level courses. Admission to the Master of Science in Cyber Security requires a baccalaureate degree from a regionally accredited institution.

The Master of Science in Cyber Security requires 30 credit hours that includes 9 hours of core courses and 21 credit hours of elective courses. Graduation requires 30 credit hours. Students can choose a thesis or non-thesis options.

International applicants must submit a satisfactory GMAT and TOEFL score in order to be considered for admission.

The Cyber Security applicants must submit (1) curriculum vitae or resume, (2) one-page essay on student's aspirations and the reason student wants to complete the MS-CSEC program, (3) One letter of recommendation.

Graduate Admissions Required Test Scores

Students with an undergraduate major in computer science or related fields with an average GPA of 3.0/4.0 or better on all prior advanced-level (junior, senior, and graduate) math and computer science-related work taken from an accredited institution. Students below an average GPA of 3.0 but greater than 2.5 may be granted conditional admission.

Entrance Exams Waived FALL 2023

The required GMAT Score is 450 or an equivalent GRE score of 298 will also suffice (waived for academic year 2022-2023).
Texas A&M University-San Antonio Graduate Management Admissions Test (GMAT) code: 7B7-9D-05

Texas A&M University-San Antonio Graduate Record Exam (GRE) code: 6712

Application Instructions

Complete the GradCAS application and submit the appropriate fees and required documentation. Request official e-transcripts from all US institutions attended to be sent to GradCAS through the GradCAS online order portal. If your institution does not have official e-transcripts available, they can be mailed to the GradCAS processing center.

GradCas Link: Apply | GradCAS (liaisoncas.org) (https://gradcas.liaisoncas.org/apply/)

For questions or assistance, email: Cyber@tamusa.edu

***Failure to list all colleges and universities on your application will delay processing for admission. **Official transcripts must be sent to GradCAS. ***Do not send transcripts to Texas A&M - San Antonio.**

Credentialing reports of transcripts from all foreign institutions can be sent electronically through the World Education Services (WES) link in the Academic History section of the application or by mail if using another credentialing agency.

International applicants must demonstrate English proficiency by scoring a minimum TOEFL score of 550 (paper-based), 213 (computer-based) or 79 (Internet-based). The TOEFL school code is 6712.

Admission Deadlines

Fall 2023:

- Priority: 2/1/2023
- Regular: 5/20/2023
- Late: 7/15/2023

Requirements

Curricula

The program consists of 9 semester credit hours of required Cyber Security (CSEC) core courses and 21 semester credit hours of graduate CSEC electives.

Code	Title	Credits
Required MS Cyber Security Core Courses		**9**
CSEC 5310	Advanced Topics in Computer Forensics	3
CSEC 5321	Information Assurance and Risk Management	3
CSEC 5327	Advanced Information Security	3
Elective Courses		**21**
Select 21 credits of electives based on career goals/focus and approval by advisor.		
CSEC 5300	Research Seminar	3
CSEC 5304	Database Security	3
CSEC 5306	Computer Networks and Security	3
CSEC 5311	Big Data Analysis and Security	3
CSEC 5322	Identity Management and Access Control	3
CSEC 5323	Cryptography and Secure Communication	3
CSEC 5326	Security in Emerging Technologies	3
CSEC 5333	Programming for Cyber Security	3
CSEC 5350	Intrusion Detection and Hackers Exploits	3
CSEC 5370	Special Topics in Cyber Security	3
CSEC 5380	Cyber incident response	3
Total Credits		**30**

Plan of Study

This suggested plan of study is intended to be used as a guide in conjunction with the official degree requirements outlined in the catalog. While this plan

demonstrates a course of study that covers four semesters, each student's academic path is unique, and your timeline may look different. Electives listed in the plan of study should be selected based on the student's career goals/ focus and approved by their advisor.

First Year		
First Semester		**Credits**
CSEC 5310	Advanced Topics in Computer Forensics	3
CSEC 5321	Information Assurance and Risk Management	3
CSEC 5327	Advanced Information Security	3
	Credits	**9**
Second Semester		
Elective		3
Elective		3
Elective		3
	Credits	**9**
Third Semester		
Elective		3
	Credits	**3**
Second Year		
First Semester		
Elective		3
Elective		3
Elective		3
	Credits	**9**
	Total Credits	**30**