CYBER SECURITY ENGINEERING, MS

Banner Code: EC-MS-CYSE

Phone: 703-993-6760
Email: cysegrad@gmu.edu
Website: https://cybersecurity.sitemasonry.gmu.edu/academics/master-science-cyber-security-engineering

The field of cyber security engineering is concerned with the development of cyber-resilient systems that include the protection of physical as well as computer and network systems. It requires a holistic and proactive approach in engineering the design of systems, with cybersecurity incorporated from the beginning of system development all the way throughout the system's life cycle.

The purpose of the MS in Cyber Security Engineering is to provide students with the currently rare combination of highly technical knowledge and skills, cyber security expertise, and a comprehensive systems engineering perspective. The program provides theory and practice on the design, planning, and management of systems and procedures for protecting critical physical and cyber infrastructure from external threats, including terrorism. Students will be equipped with deep technical foundations of cyber security in the form of software, hardware, networking, and cryptography, as well as systems engineering tools and methods to design and secure complex cyber physical systems. Topics in the program include homeland security policies, critical infrastructure policies, information assurance cybersecurity quantification, matrix vulnerability assessment, threat assessment, physical security, personnel security, operational security, contingency planning, case analyses of specific industries and systems, redundancy planning, emergency and disaster planning, security systems, and intelligence operations.

Graduates are prepared to design and implement secure complex and cyber-physical systems consisting of software, hardware, and networking components; respond to, investigate, and remediate incidents involving these systems; and develop offensive and defensive tools and techniques to attack and secure these systems.

At the doctoral level, the department offers a concentration in the PhD in Information Technology (https://catalog.gmu.edu/colleges-schools/engineering-computing/information-technology-phd/) program.

Admissions & Policies

Admissions

The MS in Cyber Security Engineering will build on the body of knowledge acquired in undergraduate programs of study in engineering, computer science, or closely related disciplines. As such, applicants will be expected to have a bachelor's degree in engineering, computer science, or closely related disciplines and to have completed the engineering math sequence as well as courses in probability and statistics, and computer science. A minimum undergraduate GPA of 3.00 is required. Application Requirements and Deadlines are available from https://cec.gmu.edu/admissions/graduate-admissions/application-requirements-and-deadlines (https://cec.gmu.edu/admissions/graduate-admissions/application-requirements-and-deadlines/).

Domestic students lacking a working background in engineering mathematics and computer systems may be admitted provisionally and required to take one or more foundation courses.

- For the engineering mathematics, the department may require SYST 500 Quantitative Foundations for Systems Engineering or an equivalent course with an intensive review of undergraduate engineering mathematics, including matrix algebra, calculus, differential equations, probability and statistics.
- Students who have not completed a two-semester calculus sequence and matrix algebra will be required to complete these courses prior to taking SYST 500
- For the computer systems background, the department may require CS 531 Computer Systems and Fundamentals of Systems Programming or an equivalent course with systems level of programming with an emphasis on data structures and interfacing with operating systems.

Policies

Please see AP.6. Graduate Policies (https://catalog.gmu.edu/policies/academic/graduate-policies/).

Students must complete a minimum of 30 graduate credits beyond the bachelor's degree with a GPA of 3.00 or higher, inclusive of core coursework, elective courses and a mandatory capstone or thesis.

Requirements

Degree Requirements

Total credits: 30

Required Core Coursework

Code	Title	Credits
CYSE 550	Cyber Security Engineering Fundamentals	3
Students who completed the BS CYSE program at George Mason should take CYSE 630, CYSE 640, CYSE 670, or CYSE 689 instead of CYSE 550		
CYSE 570	Fundamentals of Operating Systems	3
CYSE 580	Hardware and Cyber Physical Systems	3
CYSE 587	Cyber Security Systems Engineering	3
CYSE 610	Networks and Cyber Security	3
Total Credits		**15**

No Concentration

Code	Title	Credits
Electives		
Select four courses from the following (only one non-CYSE course is permitted):		12
AIT 670	Cloud Computing Security	
CYSE 521	Industrial Control Systems Security	
CYSE 650	Topics in Cyber Security Engineering	
CYSE 670	Secure Design of Connected and Automated Vehicles	

CYSE 680	Advanced Manufacturing Automation Security
CYSE 681	Secure Energy Efficient Supply Chains
CYSE 682	Formal Methods for Cyber Physical Systems Security
CYSE 683	Reverse Engineering Industrial Automation
CYSE 684	Practical Side-Channel Exploitation and Defense
CYSE 685	Unmanned Aerial Systems Security
CYSE 686	Introduction to Federated Learning: Fundamentals and Applications
CYSE 689	Artificial Intelligence Methods for Cybersecurity
CYSE 698	Independent Study and Research
CYSE 750	Advanced Topics in Cyber Security Engineering
ECE 547	Applied Cryptography
ECE 554	Machine Learning for Embedded Systems
ECE 647	Post-Quantum Cryptography
ECE 649	Side-Channel Security
ECE 570	Quantum Computing System Design
DFOR 761	Malware Reverse Engineering
DFOR 767	Penetration Testing in Digital Forensics
DFOR 775	Kernel Forensics and Analysis
SYST 548	Technologies and Security for Cryptocurrencies and Financial Transactions
Total Credits	**12**

Concentration in Secure Advanced Manufacturing and Supply Chains (SAMS)

Code	Title	Credits
Required		
CYSE 680	Advanced Manufacturing Automation Security	3
CYSE 681	Secure Energy Efficient Supply Chains	3
Electives		
Select two courses from the following:		6
CYSE 521	Industrial Control Systems Security	
CYSE 630	Cyber Risk Analysis and Advanced Tools	
CYSE 650	Topics in Cyber Security Engineering	
CYSE 682	Formal Methods for Cyber Physical Systems Security	
CYSE 683	Reverse Engineering Industrial Automation	
CYSE 684	Practical Side-Channel Exploitation and Defense	
CYSE 686	Introduction to Federated Learning: Fundamentals and Applications	
CYSE 689	Artificial Intelligence Methods for Cybersecurity	
CYSE 731	Graphical Models for Cybersecurity	
Total Credits		**12**

Concentration in Autonomous Vehicles Cyber Security (AVCS)

Code	Title	Credits
Required		
CYSE 640	Wireless Network Security	3
CYSE 670	Secure Design of Connected and Automated Vehicles	3
or CYSE 685	Unmanned Aerial Systems Security	
Electives		
Select two courses from the following:		6
CYSE 630	Cyber Risk Analysis and Advanced Tools	
CYSE 650	Topics in Cyber Security Engineering	
CYSE 670	Secure Design of Connected and Automated Vehicles	
CYSE 682	Formal Methods for Cyber Physical Systems Security	
CYSE 683	Reverse Engineering Industrial Automation	
CYSE 684	Practical Side-Channel Exploitation and Defense	
CYSE 685	Unmanned Aerial Systems Security	
CYSE 686	Introduction to Federated Learning: Fundamentals and Applications	
CYSE 689	Artificial Intelligence Methods for Cybersecurity	
CYSE 731	Graphical Models for Cybersecurity	
Total Credits		**12**

Concentration in Cyber Secure Artificial Intelligence Systems (CSAI)

Code	Title	Credits
Required		
CYSE 686	Introduction to Federated Learning: Fundamentals and Applications	3
CYSE 689	Artificial Intelligence Methods for Cybersecurity	3
Electives		
Select two courses from the following:		6
CYSE 630	Cyber Risk Analysis and Advanced Tools	
CYSE 650	Topics in Cyber Security Engineering	
CYSE 682	Formal Methods for Cyber Physical Systems Security	
CYSE 683	Reverse Engineering Industrial Automation	
CYSE 731	Graphical Models for Cybersecurity	
ECE 651	Advanced Learning From Data	
ECE 653	Machine Learning Security and Privacy	
Total Credits		**12**

Capstone Project or Thesis (3-6 credits):

Students must complete three credit hours of CYSE 690 Cyber Security Engineering Capstone Project. In this course, students collaborate in teams to analyze and design a comprehensive cybersecurity system that integrates software, hardware, and human components. This course applies cybersecurity engineering principles to the system's design,

implementation, and operation. Key elements of this course encompass requirements analysis, evaluation of design alternatives, threat and risk assessment, and economic and regulatory considerations. The course demands both oral and written reports throughout its duration.

Optionally, students with the consent of a faculty adviser, the formation of a thesis committee, and departmental approval may be approved to complete the CYSE 799 Cyber Security Engineering Master's Thesis (https://catalog.gmu.edu/search/?scontext=courses&search=CYSE+799) in place of the Capstone Project. The thesis option is recommended for students aiming to enhance and document their research skills or considering future enrollment in a PhD program. To pursue this option, students must obtain approval from a full-time faculty member who will serve as their thesis advisor. The thesis topic and scope require the thesis advisor's approval. The completed thesis and its oral defense are subject to approval by the student's advisory committee.

Please see AP.6.9.3 (https://catalog.gmu.edu/policies/academic/graduate-policies/#ap-6-9-3) for additional information.

Accelerated Master's

Cyber Security Engineering, BS/Cyber Security Engineering, Accelerated MS

Overview

Highly-qualified undergraduates may be admitted to the bachelor's/accelerated master's program and obtain a BS in Cyber Security Engineering (https://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/cyber-security-engineering-bs/) and an MS in Cyber Security Engineering in an accelerated time-frame after satisfactory completion of a minimum of 144 credits.

See AP.6.7 Bachelor's/Accelerated Master's Degree (https://catalog.gmu.edu/policies/academic/graduate-policies/#ap-6-7) for policies related to this program.

This accelerated option is offered by the Department of Cyber Security Engineering (https://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/).

Students in an accelerated degree program must fulfill all university requirements for the master's degree. For policies governing all graduate degrees, see AP.6 Graduate Policies (https://catalog.gmu.edu/policies/academic/graduate-policies/).

BAM Pathway Admission Requirements

Applicants to all graduate programs at George Mason University must meet the admission standards and application requirements for graduate study as specified in Graduate Admissions Policies (https://catalog.gmu.edu/admissions/graduate-policies/) and Bachelor's/Accelerated Master's Degree policies (https://catalog.gmu.edu/policies/academic/graduate-policies/#ap-6-7).

Students will be considered for admission into the BAM Pathway after completion of a minimum of 60 credits with an overall GPA of 3.5.

Students who are accepted into the BAM Pathway will be allowed to register for graduate level courses after successful completion of a minimum of 75 undergraduate credits and course-specific prerequisites.

Accelerated Master's Admission Requirements

Students already admitted in the BAM Pathway will be admitted to the MS program, if they have met the following criteria, as verified on the Bachelor's/Accelerated Master's Transition form:

- 3.0 overall GPA,
- successfully meeting Mason's requirements for undergraduate degree conferral (graduation),
- and completing the application for graduation.

Accelerated Pathway Requirements

To maintain the integrity and quality of both the undergraduate and graduate degree programs, undergraduate students interested in taking graduate courses must choose from the following:

Advanced Standing Courses

Students may take up to 12 credits of graduate-level courses that will count as advanced standing (i.e., overlap between the BS/MS program) from the list below:

Code	Title	Credits
CYSE 521	Industrial Control Systems Security	3
CYSE 570	Fundamentals of Operating Systems	3
CYSE 580	Hardware and Cyber Physical Systems	3
CYSE 587	Cyber Security Systems Engineering	3

These courses may be used as technical electives in the Cyber Security Engineering, BS (https://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/cyber-security-engineering-bs/) program.

For more detailed information on coursework and timeline requirements, see AP.6.7 Bachelor's/Accelerated Master's Degree policies (https://catalog.gmu.edu/policies/academic/graduate-policies/#ap-6-7).

Degree Conferral

Students must apply to graduate the semester before they expect to complete all BS requirements. In addition, at the beginning of the student's final undergraduate semester, students must complete a Bachelor's/Accelerated Master's Transition form. At the completion of all MS requirements, a master's degree is conferred.