

M.S. in Cyber Security

Program Goals and Objectives

With the growing demand for expertise in Cyber Security, the Master of Science in Cyber Security (MS-SEC) provides a foundation in computing and security. The program balances technical expertise with its application in industry and government spaces. The program uses real-world experiential learning and research opportunities to ensure students are prepared for an evolving threat landscape.

Admissions Requirements

Applicants are expected to demonstrate sufficient background in computing for graduate-level work. Background in developing or using software tools is required. A bachelor's degree in Computer Science, Electrical Engineering, Information Technology, or other related fields should be adequate preparation. Students from other backgrounds are welcome to apply if they can demonstrate their readiness through other means, such as GRE exams, professional certifications, or relevant technical work experience.

Applicants must have earned the equivalent of a four-year U.S. bachelor's degree to be considered for admission. Admission decisions are based upon all the information required from the applicant. The GRE is not required for admission.

Non-matriculated students may enroll in up to two courses prior to applying for admission to the Master of Science in Cyber Security.

Faculty Contacts:

Andrew Clark, Lorenzo De Carli, Yarkin Doroz, Daniel Dougherty, Fatemeh Ganji, William Martin, Koksai Mus, Patrick Schaumont, Craig Shue, Berk Sunar, Robert Walls, and Craig Wills.

Requirements for the Master of Science in Cyber Security (MS-SEC)

The Master of Science in Cyber Security allows students to pursue research or focus on applied courses that address security problems. Students may choose to complete either a capstone project or a MS thesis. The degree requires at least 30 credits hours of study, i.e., a minimum of ten 3-credit courses.

The MS-SEC is designed to accommodate students with significant prior preparation as well as those seeking to become professionals in the field. It supports both a standard and an advanced track of study. These tracks are for advising purposes only; students on either track earn the same credential and the selected track is not officially

recorded. Under each track, students are encouraged to focus on either a software-centric or hardware-centric collection of courses.

Type: Master of Science

MS-SEC students may take up to three bridge courses from:

Item #	Title	Credits
CS 5007	Introduction to Applications of Computer Science with Data Structures and Algorithms	3
CS 5008	Introduction to Systems and Network Programming	3
CS 509	Design of Software Systems	3

MS-SEC students must complete a three-course core focused on technical, human behavior, and business:

- One technically-focused course from:

Item #	Title	Credits
CS 557	Software Security Design and Analysis	3
CS 558	Computer Network Security	3
DS/ECE 577	Machine Learning in Cybersecurity	3
	ECE 579S Computer Security	
	ECE 579C Applied Cryptography and Physical Attacks	

- One human behavior-focused course from:

Item #	Title	Credits
CS 571	Case Studies in Computer Security	3
	CS 525 Digital Forensics	
	CS 525 Computer Crime Law	
	ECE 579B Blockchain and Cryptocurrencies	

- MIS 582 Information Security Management

Item #	Title	Credits
MIS 582	Information Security Management	3

MS-SEC students must complete three depth courses from the following:

Item #	Title	Credits
CS 578/ECE 578	Cryptography and Data Security	3
CS 673/ECE 673	Advanced Cryptography	3
CS 564	Advanced Topics in Computer Security	3
OIE 542	Risk Management and Decision Analysis	3
Any core course from above that has not been used to satisfy the core requirement.		

In the standard track, our bridge component supports students with less preparation to help them learn core concepts needed in subsequent classes. While highly recommended for those without previous technical preparation related to the field, these courses are optional preparation. Students who already have significant preparation in these areas, through undergraduate classes, graduate classes, or professional experience may choose not to take one or more bridge course without requiring advisor or program approval. For students on the software-centric standard track, CS 5007, CS 5008, and CS 509 are useful preparation.

In the advanced track, students may choose not to take any of the bridge courses and instead focus on technical depth or electives. Students on the advanced software-centric track may prefer to take either CS 557 or CS 558. Students on the advanced hardware-centric track may prefer to take DS/ECE 577 Machine Learning in Cybersecurity or ECE 579C Applied Cryptography and Physical Attacks.

MS-SEC students who do not take all of the bridge courses may select to take thesis credits or additional elective courses from the following to reach the 30-credit requirement:

Item #	Title	Credits
CS 502	Operating Systems	3
CS 513	Computer Networks	3
CS 534	Artificial Intelligence	3
CS 539	Machine Learning	3
CS 542	Database Management Systems	3
CS 546	Human-Computer Interaction	3
CS 548	Knowledge Discovery and Data Mining	3
CS 573	Data Visualization	3
ECE 506	Introduction to Local and Wide Area Networks	3
ECE 5307	Wireless Access and Localization	3
Undergraduate courses through the BS/MS program that have significant material overlap with the above graduate courses, as specified in the following section.		
Any core or depth course from above that has not been used to satisfy either the core or depth requirements.		