

MASTER OF SCIENCE IN CYBERSECURITY

The Master of Science in Cybersecurity degree program requires 32 credit hours of coursework (including a 5 credit practicum project course). Two of the core courses, which students in each specialization will take, will provide a broad overview of technology and policy dimensions of cybersecurity. Students are required to take a third core course that comes from one of the other specializations; e.g., a policy specialization student must take a course from the cyber-physical or information security track. Finally, a practicum project (5 credit hours) with common learning objectives across all participating units will be a core requirement. Each participating unit will decide required and elective courses for the MS Cybersecurity degree specialization offered by it (a total of 18 credit hours). These requirements have been defined by the participating units and are described in the next section.

Although all three participating schools will offer a single degree, MS Cybersecurity, the focus of the degree will depend on the specialization defined by the offering unit. In particular, each unit will offer the following specializations for the MS degree in Cybersecurity.

- The School of Cybersecurity and Privacy (SCP) offers the MS Cybersecurity degree with an information security specialization.
- The School of Electrical and Computer Engineering (ECE) offers the MS Cybersecurity degree with cyber-physical systems specialization.
- The School of Public Policy (PUBP) offers the MS cybersecurity degree with a policy specialization.

Program of Study

Code	Title	Credit Hours
Required Core Courses:		
CS 6035	Introduction to Information Security	3
PUBP/CS/MGT 6725	Information Security Policies and Strategies	3
CS/ECE/PUBP 6727	Cyber Security Practicum	5
Elective course	CS/PUBP/ECE 6000-level ¹	3
Specialization Requirements (see below for specialization specific requirements)		18
Total Credit Hours		32

¹ Public Policy students must take CS or ECE elective

GPA/Grade Requirements:

- Students must achieve a grade-point average of at least 3.0 to graduate
- No course grades below 'C' will count toward graduation
- Students must take all master's degree coursework on a letter-grade basis

Code	Title	Credit Hours
Information Security Specialization:		
CS 6260	Applied Cryptography	3

CS 6238	Secure Computer Systems	3
CS 6262	Network Security	3
CS 6265	Information Security Laboratory	3
or CS 6264 Information Security Lab: System and Network Defenses		
or CS 6747 Advanced Topics in Malware Analysis		
Any graduate level CS numbered courses ¹		6
Total Credit Hours		18

¹ Any graduate level CS numbered courses (CS 6xxx or CS 7xxx). CS 8803 courses require program coordinator approval. No more than one CS 8903 can be used to satisfy this requirement.

Code	Title	Credit Hours
Cyber-Physical Systems Specialization:		
Select 4 Courses:		12
ECE 6156	Hardware-Oriented Security and Trust	
ECE 6320	Power Systems Control and Operation	
ECE 6374	Cyber-Physical Security in Electric Energy Systems	
ECE 8813	Special Topics (Introduction to Cyber-Physical Systems Security)	
ECE 8803	Special Topics (Cybersecurity of Drones)	
ECE 8823	Special Topics (Cyber Physical Design and Analysis)	
Select 2 courses:		6
ECE 6550	Linear Systems and Controls	
ECE 6607	Computer Communication Networks	
ECE 6615	Sensor Networks	
ECE 6102	Dependable Distributed Systems	
ECE 6323	Power System Protection	
ECE 8813	Special Topics (Advanced Computer Security)	
ECE 8813	Special Topics (Network Forensics)	
ECE 8813	Special Topics (Smart Grids)	
ECE 6747	Advanced Topics in Malware Analysis	
ECE 6100	Advanced Computer Architecture	
ECE 6254	Statistical Machine Learning	
ECE 6273	Methods of Pattern Recognition with Application to Voice	
ECE 6562	Autonomous Control of Robotic Systems	
ECE 6563	Networked Control and Multiagent Systems	
ECE 6601	Random Processes	
ECE 6612	Computer Network Security	
or CS 6262 Network Security		
ECE 6610	Wireless Networks	
ECE 6615	Sensor Networks	
ECE 6780	Medical Image Processing	
ECE 6790	Information Processing Models in Neural Systems	
ECE 7142	Fault Tolerant Computing	
ECE 8803	Special Topics (Empirical Computer Security)	
ECE 8843	Special Topics (Side Channels and Their Role in Cybersecurity)	

ECE 8893	Special Topics-Laboratory (Parallel Programming for FPGAs)	
CS 6263	Intro to Cyber-Physical Systems Security	
CS 8803	Special Topics (Critical Infrastructure Security)	
Total Credit Hours		18
Code	Title	Credit Hours
Policy Specialization:		
Select 4 courses:		12
CS 8803	Special Topics (Security Operations and Incident Response)	
INTA 6014	Scenario Writing and Path Gaming	
INTA 6103	International Security	
INTA 6450	Data Analytics and Security	
MGT/CS/ PUBP 6726	Privacy, Technology, Policy, and Law	
PUBP 6111	Internet and Public Policy	
PUBP 6501	Information Policy and Management	
PUBP 6502	Information and Communications Technology Policy	
Electives ¹		6
Total Credit Hours		18

¹ Free electives which may be satisfied by courses from any of the specializations

The Master of Science in Cybersecurity is also offered online.

For more information, visit: [Online Master of Science in Cybersecurity](#).