

M.S. IN CYBER SECURITY

OVERVIEW

Weiqing Sun, program director

Our master's degree programs in cyber security provide an experiential learning-rich curriculum tailored to your interests and industry's needs. The programs offer personalized capstone options and a large number of elective courses, prepares you for research and development jobs in cyber security areas, and provides a foundation for carrying out cyber security research and development. Flexible course scheduling within our programs enables you to start taking classes during either fall or spring semester. We offer a research-based Master of Science in Cyber Security and a coursework-based Master in Cyber Security. You can pick the degree that best fits with your professional goals and interests.

Master of Science in Cyber Security is our research-intensive degree program, and it offers two capstone options (thesis or project) for you to work on cyber security research projects under the guidance of a faculty research mentor. This program helps you develop skills to investigate cyber security issues, discover new cyber security knowledge and present your research to professionals in the industry or academia. After completing this program, you will be prepared to continue your research and development in cyber security areas or work in industry, practicing learned professional skills. You will be required to take 30 credit hours to graduate.

For more information, please check the program website (<https://www.utoledo.edu/engineering/graduate-studies/cyber.html>) and contact the Program Director (Dr. Weiqing Sun, weiqing.sun@utoledo.edu).

ADMISSIONS REQUIREMENTS

Prospective students must have a bachelor's degree with a minimum 3.0/4.0 GPA or equivalent in a computer science or related field. For other STEM graduates, prerequisite undergraduate-level foundation courses in computer programming, computer networks, data structures, and operating systems are required. University of Toledo equivalent courses are shown below.

Code	Title	Hours
<i>Programming - one course or equivalent</i>		
CSET 1200	Object Oriented Programming and Data Structures	
EECS 1510	Introduction To Object Oriented Programming	
<i>Computer Networks - one course or equivalent</i>		
CSET 4750	Computer Networks And Data Communication	
EECS 3150	Data Communications	
<i>Data Structures and Algorithms - one course or equivalent</i>		
CSET 3150	Introduction to Algorithms	
EECS 2510	Non-Linear Data Structures	
<i>Operating Systems - one course or equivalent</i>		
CSET 4350	Operating Systems	
EECS 3540	Systems And Systems Programming	

The application requires transcripts from all universities attended (except UToledo); 3 letters of recommendation, with at least one from an

employer or a professor; a personal statement written in response to a cyber security prompt; current GRE score; and TOEFL score for students with a BS degree from a non-US institution.

PROGRAM REQUIREMENTS

Thesis option:

Code	Title	Hours
Core Courses		(10 cr hr)
EECS 5760	Computer Security	
EECS 5720	Essentials of Cyber Security	
EECS 5790	Network Security	
Engineering Elective Courses		(8 cr hr)
EECS 5640	Inside Cryptography	
EECS 5770	Computer Hacking and Forensic Analysis	
EECS 6650	Hardware Oriented Security and Trust	
EECS 5520	Advanced Systems Programming	
CYBR 5930	Cyber Security Seminar	
CYBR 6990	Independent Study in Cyber Security	
CYBR 6800	Experiential Learning in Cyber Security	
CYBR 6970	Graduate Engineering Internship	
<i>Select up to one of the following:</i>		
EECS 5500	Programming for the World Wide Web	
EECS 5740	Artificial Intelligence	
EECS 5750	Machine Learning	
EECS 6180	Biologically Inspired Computing	
EECS 6350	Modern Communications Engineering II	
Non-Engineering Elective Courses		(3 cr hr)
INFS 6710	Management of Information Systems Security	
LAWT 6600	Special Topics (Privacy and Data Security (College of Law, spring))	
LAWI 6290	(Cyberspace Laws (College of Law, fall))	
Capstone		(9 cr hr)
CYBR 6960	Cyber Security Research and Thesis	

Project option:

Code	Title	Hours
Core Courses		(10 cr hr)
EECS 5760	Computer Security	
EECS 5720	Essentials of Cyber Security	
EECS 5790	Network Security	

Engineering Elective Courses (11 cr hr)

EECS 5640	Inside Cryptography	
EECS 5770	Computer Hacking and Forensic Analysis	
EECS 6650	Hardware Oriented Security and Trust	
EECS 5520	Advanced Systems Programming	
CYBR 5930	Cyber Security Seminar	
CYBR 6990	Independent Study in Cyber Security	
CYBR 6800	Experiential Learning in Cyber Security	
CYBR 6970	Graduate Engineering Internship	

Select up to one of the following:

EECS 5500	Programming for the World Wide Web	
EECS 5740	Artificial Intelligence	
EECS 5750	Machine Learning	
CYBR 6970	Graduate Engineering Internship	
EECS 6180	Biologically Inspired Computing	
EECS 6350	Modern Communications Engineering II	

Non-Engineering Elective Courses (3 cr hr)

INFS 6710	Management of Information Systems Security	
LAWT 6600	Special Topics (Privacy and Data Security (College of Law, spring))	
LAWI 6290	(Cyberspace Laws (College of Law, fall))	

Capstone (6 cr hr)

CYBR 6920	Cyber Security Project	
-----------	------------------------	--

First Year

First Term		Hours
EECS 5720	Essentials of Cyber Security	3
EECS 5760	Computer Security	3
EECS 5750	Machine Learning	3
CYBR 5930	Cyber Security Seminar	0
Hours		9

Second Term

EECS 5640	Inside Cryptography	3
EECS 5790	Network Security	4
CYBR 6990	Independent Study in Cyber Security	2
CYBR 5930	Cyber Security Seminar	0
Hours		9

Second Year

First Term		Hours
CYBR 6920	Cyber Security Project	3
CYBR 6800	Experiential Learning in Cyber Security	3
LAWI 6290	Cyberspace Laws	3
CYBR 5930	Cyber Security Seminar	0
Hours		9

Second Term		Hours
CYBR 6920	Cyber Security Project	3
CYBR 5930	Cyber Security Seminar	0
Hours		3
Total Hours		30

First Year		Hours
First Term		
EECS 5720	Essentials of Cyber Security	3
EECS 5760	Computer Security	3
LAWI 6290	Cyberspace Laws	3
CYBR 5930	Cyber Security Seminar	0
Hours		9

Second Term		Hours
EECS 5640	Inside Cryptography	3
EECS 5790	Network Security	4
CYBR 6990	Independent Study in Cyber Security	2
CYBR 5930	Cyber Security Seminar	0
Hours		9

Third Term		Hours
CYBR 6960	Cyber Security Research and Thesis	1
Hours		1

Second Year		Hours
First Term		
EECS 5750	Machine Learning	3
CYBR 6960	Cyber Security Research and Thesis	6
CYBR 5930	Cyber Security Seminar	0
Hours		9

Second Term		Hours
CYBR 6960	Cyber Security Research and Thesis	2
CYBR 5930	Cyber Security Seminar	0
Hours		2
Total Hours		30

- Understand the cyber security challenges in contemporary networks and software systems.
- Demonstrate the proficiency in various tools and utilities used in cyber security.
- Evaluate security mechanisms in terms of their effectiveness and appropriateness for computer and network systems.
- Understand the ethical issues related to securing information systems and critical infrastructure.
- Communicate effectively, both orally and in writing, with other security professionals.
- Apply appropriate security methods and mechanisms to protect enterprise network systems.
- Research cyber security issues, discovery new knowledge, and present the research results to professionals in industry or academia.