Master of Science (MS) in Cybersecurity Engineering

The Master of Science (MS) in Cybersecurity Engineering at Washington University will give students the skills, knowledge and expertise needed to work in the rapidly growing field of cybersecurity and to design, engineer and architect cybersecurity technology and systems. Graduates of this program will be equipped with the theoretical and hands-on engineering expertise required to solve complex cybersecurity problems that affect diverse enterprises worldwide.

The program includes a set of core foundational courses that focus on operating systems as well as network and systems security. Students pursuing this degree may also choose from more advanced cybersecurity elective courses that will build deeper integrative knowledge of key concepts. Work in the program culminates in either a capstone project or a final thesis. The capstone project should focus on a specific set of technical cybersecurity challenges, with the objective of designing an implementable solution to those challenges. The thesis option allows students to plan, execute and report on an individual project that addresses a substantial problem, covering both practical and scientific aspects. Students planning to pursue a PhD degree after completing the MS in Cybersecurity degree are particularly encouraged to pick the thesis option.

All students in the MS in Cybersecurity Engineering program must have previously completed (as documented by their undergraduate transcript), successfully tested to place out of, or completed at the start of their program the following courses: CSE 501N Introduction to Computer Science and CSE 502N Data Structures and Algorithms (or equivalent courses offered at other institutions).

Core Courses

Code	Title	Units
CSE 422S	Operating Systems Organization	3
CSE 433S	Introduction to Computer Security	3
CSE 473S	Introduction to Computer Networks	3
CSE 523S	Systems Security	3
Total Units		**12**

Program Electives

Choose three courses:

Code	Title	Units
CSE 434S	Reverse Engineering and Malware Analysis	3
CSE 522S	Advanced Operating Systems	3
CSE 544T	Special Topics in Computer Science Theory	3
CYBER 565	Cybersecurity Analytics	3
CYBER 566	Cybersecurity Risk Management	3
CYBER 567	The Hacker Mindset: Cyber Attack Fundamentals	3
CSE 569S	Recent Advances in Computer Security and Privacy	3
CSE 571S	Network Security	3
CSE 637S	Software Security	3

Culminating Experience

Choose one of the following:

Code	Title	Units
CSE 598	Master's Project	6
CSE 599	Master's Research	6
(6 units required, typically completed over the course of two semesters)		

General Degree Requirements

- Students who have already taken core or elective courses specified by the program can, with departmental approval, substitute other courses that are suitably technical and appropriate to the degree program. Departmental approval will require justification and will be evaluated with increasing stringency for each additional substitution.
- None of of the 30 units may be taken as independent study (i.e., CSE 400 or CSE 500).
- Courses with an "N" designation do not count toward the master's degree.
- All courses must be taken for a grade of C- or better.
- As per McKelvey School of Engineering guidelines, students must maintain a grade-point average of at least 2.70.