Master of Science in Cybersecurity Engineering

The Master of Science (MS) in Cybersecurity Engineering at Washington University will give students the skills, knowledge and expertise 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 to solve complex cybersecurity problems affecting diverse enterprises worldwide.

The program includes a set of core foundational courses focusing on operating systems as well as network and systems security. Students pursing 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 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 test to place out of, or complete at the start of their program, the following courses:

- CSE 501N Introduction to Computer Science
- CSE 502N Data Structures and Algorithms

Core Courses

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE 422S</td>
<td>Operating Systems Organization</td>
<td>3</td>
</tr>
<tr>
<td>CSE 433S</td>
<td>Secure Software Engineering</td>
<td>3</td>
</tr>
<tr>
<td>CSE 469S</td>
<td>Security of the Internet of Things and Embedded System Security</td>
<td>3</td>
</tr>
<tr>
<td>CSE 473S</td>
<td>Introduction to Computer Networks</td>
<td>3</td>
</tr>
<tr>
<td>CSE 523S</td>
<td>Systems Security</td>
<td>3</td>
</tr>
<tr>
<td>Total Units</td>
<td></td>
<td>15</td>
</tr>
</tbody>
</table>

Program Electives

Choose three courses:

- Advanced Operating Systems (CSE 522S)
- Advanced Secure Software Engineering (CSE 543S)
- Advanced IoT, Real-Time, and Embedded Systems Security (CSE 569S)
- Network Security (CSE 571S)
- Cybersecurity Analytics (T81 INFO 565)
- Cybersecurity Risk Management (T81 INFO 566)

Culminating Experience

Choose one of the following:

- Master's Project (CSE 598) 6 units
- Master's Research (CSE 599) 6 units

(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 shall be evaluated with increasing stringency for each additional substitution.
- None 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 Engineering School guidelines, students must maintain a GPA of at least 2.70.