MASTER OF SCIENCE IN THE FIELD OF CYBERSECURITY IN COMPUTER SCIENCE

Program Overview

The master of science in the field of cybersecurity in computer science degree program was created in response to the significant and fast-growing need for technical cybersecurity experts, both nationally and internationally. Students in the program acquire up-to-date knowledge and skills in cybersecurity, a field with increasing importance to national security, the economy, and private citizens. Students take courses in computer security, software security, network security, cryptography, and security management, among others. They also gain a firm grounding in computer science and take courses in related disciplines such as cybersecurity law and digital forensics.

Specific admission requirements are shown on the Graduate Program Finder. (http://www.gwu.edu/all-graduate-programs)

Visit the program website (http://www.cs.seas.gwu.edu/master-science-cybersecurity-computer-science) for additional information.

Prerequisites:

In addition to the entrance requirements, students are expected to be adequately prepared in the basic physical sciences and in mathematics (one year each of university laboratory science and of math beyond precalculus). Students are also expected to have taken a course in computer programming using a structured language, as well as CSCI 1112 Algorithms and Data Structures, CSCI 1311 Discrete Structures I, and CSCI 2461 Computer Architecture I, or their equivalents.

Educational Planner:

In consultation with an academic advisor, each student must develop an Educational Planner through DegreeMAP that governs the student's degree requirements. The Educational Planner should be established soon after matriculation and must be completed before the end of the student's first semester. The Educational Planner must be approved by the advisor.

REQUIREMENTS

Credit Requirements:

- Thesis option: 30 credits are required for graduation; 6 of these credits are thesis credits
- Non-thesis option: 30 credits are required for graduation
- With department approval, students who complete the MS in the field of computer science and then enroll in the MS in the field of cybersecurity in computer science degree or vice versa can count the following core courses towards both degrees: CSCI 6212 Design and Analysis of Algorithms, CSCI 6221 Advanced Software Paradigms, and CSCI 6461 Computer System Architecture.

Graduation and Scholarship Requirements:

Students are responsible for knowing the university’s minimum GPA requirement for graduation and scholarships. Please visit the Graduation and Scholarship Requirements (http://bulletin.gwu.edu/engineering-applied-science/#graduation_requirements_ms) section on this site to read the requirements.

Students should contact the department for additional information and requirements.

Program Restrictions:

- Student’s whose admission letters state that they are required to take CSCI 6010 and CSCI 6011 are limited to EMSE 6540 Management of Information Systems and Security as their only non-CS course.
- Students required to take CSCI 6010 and CSCI 6011 must take these courses in their first semester.
- Students not required to take CSCI 6010 and CSCI 6011 may take up to three non-CS courses (9 credits) towards their degree with prior written approval from their faculty advisor.
- At least 24 of the 30 credits required for the degree must be at the 6000 level or above. As a general rule, any course taken below the 6000 level must be a Computer Science course and must be eligible to be taken for graduate credit according to the course description. Exceptions may be chosen to enhance an aspect of the student’s degree program. Any course taken that is below the 6000 level must receive prior written approval from the student’s faculty advisor.

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCI 6212</td>
<td>Design and Analysis of Algorithms</td>
<td></td>
</tr>
<tr>
<td>CSCI 6221</td>
<td>Advanced Software Paradigms</td>
<td></td>
</tr>
<tr>
<td>CSCI 6461</td>
<td>Computer System Architecture</td>
<td></td>
</tr>
<tr>
<td>EMSE 6540</td>
<td>Management of Information and Systems Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>One of the following applied cryptography courses:</td>
<td></td>
</tr>
<tr>
<td>CSCI 6331</td>
<td>Cryptography</td>
<td></td>
</tr>
<tr>
<td>CSCI 6541</td>
<td>Network Security</td>
<td></td>
</tr>
<tr>
<td>CSCI 6545</td>
<td>Software Security</td>
<td></td>
</tr>
</tbody>
</table>
One of the following computer science security courses, which may not be used to fulfill applied cryptography course requirement.

CSCI 6331 Cryptography
CSCI 6541 Network Security
CSCI 6545 Software Security
CSCI 6531 Computer Security
CSCI 6532 Information Policy
CSCI 6542 Computer Network Defense
CSCI 6547 Wireless and Mobile Security
CSCI 6548 E-Commerce Security
CSCI 8331 Advanced Cryptography
CSCI 8531 Advanced Topics in Security *
CSCI 6907 Special Topics *

Any special topics course taken for credit towards the degree must focus on security or cryptography and be approved by the faculty advisor.

Two additional security courses (6 credits) from across the university*.

All computer science security courses listed above not used to meet the applied cryptography or computer science security course requirements as well as the following courses may be used:

EMSE 6537 Information Operations
EMSE 6543 Managing the Protection of Information Assets and Systems
EMSE 6545 Internet and Online Law for Security Managers

Any other cybersecurity-related course from across the university must be reviewed and approved by the student's advisor to ensure that it is sufficiently advanced and rigorous before it can be taken for credit towards the degree.

**Electives**

Students who are not taking the thesis option and are not required to take CSCI 6010 or CSCI 6011 can choose any two additional courses (6 credits) numbered 6000 or higher.

Students who choose the thesis option must obtain the written approval of their thesis advisor before registering for the following courses:

CSCI 6998 Thesis Research

CSCI 6999 Thesis Research

If the admissions letter states that students are required to take CSCI 6010 and CSCI 6011, they will be limited to EMSE 6540 Management of Information Systems and Security as their only non-computer science course. Students required to take CSCI 6010 and CSCI 6011 are required to take these courses in their first semester. Students not required to take CSCI 6010 and CSCI 6011 may take up to three non-computer science courses (9 credits) towards their degree with prior written approval from their advisor.

At least 24 of the 30 credits required for the degree must be at the 6000 level or above. As a general rule, any course taken below the 6000 level must be a computer science course and must be eligible to be taken for graduate credit according to the course description. Exceptions may be chosen to enhance an aspect of the student’s degree program. Any course taken that is below the 6000 level must receive prior written approval from the student’s advisor.

With department approval, students who complete the Master of Science in Computer Science and then enroll in the Master of Science in the field of Cybersecurity in Computer Science or vice versa can count the following core courses towards both degrees:

CSCI 6212 Design and Analysis of Algorithms
CSCI 6221 Advanced Software Paradigms
CSCI 6461 Computer System Architecture

*Any special topics course taken for credit toward the degree must be approved by the faculty advisor and it must focus on security or cryptography.

**Any cybersecurity-related course not specifically listed here must be approved in advance by the student’s advisor to ensure it is sufficiently advanced and rigorous to count toward credit for the degree.