The field of cyber security engineering is concerned with the development of cyber-resilient systems that include the protection of physical as well as computer and network systems. It requires a proactive approach in engineering the design of systems, with cybersecurity incorporated from the beginning of system development. The purpose of the MS in Cyber Security Engineering is to provide students with the currently rare combination of highly technical knowledge and skills, cyber security expertise, and a holistic systems engineering perspective. The program provides instruction on the design, planning, and management of systems and procedures for protecting critical physical and cyber infrastructure from external threats, including terrorism. The program provides students with the deep technical foundations of cyber security in the form of software, hardware, networking, and cryptography, as well as systems engineering tools and methods to design and secure complex cyber physical systems. Students learn homeland security policy, critical infrastructure policy, information security, matrix vulnerability assessment, threat assessment, physical security, personnel security, operational security, contingency planning, case analyses of specific industries and systems, redundancy planning, emergency and disaster planning, security systems, and intelligence operations. Graduates are prepared to design and implement secure complex and cyber-physical systems consisting of software, hardware, and networking components; respond to, investigate, and remediate incidents involving these systems; and develop offensive and defensive tools and techniques to attack and secure these systems.

Admissions & Policies

Admissions

The MS in Cyber Security Engineering will build on the body of knowledge acquired in undergraduate programs of study in engineering, computer science, or closely related disciplines. As such, applicants will be expected to have a bachelor’s degree in engineering, computer science, or closely related disciplines and to have completed the engineering math sequence as well as courses in probability and statistics, and computer science. A minimum undergraduate GPA of 3.00 is required.

Policies

Students must complete a minimum of 30 graduate credits beyond the bachelor’s degree with a GPA of 3.00 or higher, with no more than 6 credit hours of C grades. The plan of study includes a 21 credit required Core component which includes a mandatory capstone course, and 9 credits of electives.

Requirements

Degree Requirements

Total credits: 30

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIT 660</td>
<td>Cyber Security Fundamentals</td>
<td>3</td>
</tr>
<tr>
<td>CS 571</td>
<td>Operating Systems</td>
<td>3</td>
</tr>
<tr>
<td>or CYSE 570</td>
<td>Fundamentals of Operating Systems</td>
<td></td>
</tr>
<tr>
<td>CYSE 580</td>
<td>Hardware and Cyber Physical Systems</td>
<td>3</td>
</tr>
<tr>
<td>CYSE 610</td>
<td>Networks and Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>ECE 646</td>
<td>Applied Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>SYST 687</td>
<td>Cybersecurity Systems Engineering</td>
<td>3</td>
</tr>
<tr>
<td>CYSE 690</td>
<td>Cybersecurity Engineering Capstone Project</td>
<td>3</td>
</tr>
</tbody>
</table>

Electives

Select three courses from the following:

- AIT 670 Cloud Computing Security
- BIOD 760 National Security Technology and Policy
- CFRS 761 Malware Reverse Engineering
- CFRS 767 Penetration Testing in Computer Forensics
- CFRS 775 Kernel Forensics and Analysis
- GBUS 540 Analysis of Financial Decisions
- ECE 527 Learning From Data
- or DAEN 527 Learning From Data
- ECE 746 Advanced Applied Cryptography
- INFS 622 Information Systems Analysis and Design
- ISA 673 Operating Systems Security
- ISA 681 Secure Software Design and Programming
- or SWE 681 Secure Software Design and Programming

Total Credits 30