Master of Science in Cyber Security (MS-SEC) - Forthcoming Graduate Catalog Entry

Program Goals and Objectives
With the growing demand for expertise in Cyber Security, the Master of Science in Cyber Security (MS-SEC) provides a foundation in computing and security. The program balances technical expertise with its application in industry and government spaces. The program uses real-world experiential learning and research opportunities to ensure students are prepared for an evolving threat landscape.

Admissions Requirements
Applicants are expected to demonstrate sufficient background in computing for graduate-level work. Background in developing or using software tools is required. A bachelor's degree in Computer Science, Electrical Engineering, Information Technology, or other related fields should be adequate preparation. Students from other backgrounds are welcome to apply if they can demonstrate their readiness through other means, such as GRE exams, professional certifications, or relevant technical work experience.

Applicants must have earned the equivalent of a four-year U.S. bachelor's degree to be considered for admission. Admission decisions are based upon all the information required from the applicant. The GRE is not required for admission.

Non-matriculated students may enroll in up to two courses prior to applying for admission to the Master of Science in Cyber Security.

Faculty Contacts: Andrew Clark, Lorenzo De Carli, Yarkin Doroz, Daniel Dougherty, Fatemeh Ganji, William Martin, Koksal Mus, Patrick Schaumont, Craig Shue, Berk Sunar, Robert Walls, and Craig Wills.

Requirements for the Master of Science in Cyber Security (MS-SEC)
The Master of Science in Cyber Security allows students to pursue research or focus on applied courses that address security problems. Students may choose to complete either a capstone project or a MS thesis. The degree requires at least 30 credits hours of study, i.e., a minimum of ten 3-credit courses.

The MS-SEC is designed to accommodate students with significant prior preparation as well as those seeking to become professionals in the field. It supports both a standard and an advanced track of study. These tracks are for advising purposes only; students on either track earn the same credential and the selected track is not officially recorded. Under each track, students are encouraged to focus on either a software-centric or hardware-centric collection of courses.

MS-SEC students may take up to three bridge courses from:

- CS 5007 Introduction to Programming Concepts, Data Structures, and Algorithms
- CS 5008 Introduction to Systems and Network Programming [**new**]

- CS 509 Design of Software Systems

MS-SEC students must complete a three-course core focused on technical, human behavior, and business:

- One technically-focused course from:
    - CS 557 Software Security Design and Analysis
    - CS 558 Computer Network Security
    - DS/ECE 577 Machine Learning in Cybersecurity
    - ECE 579S Computer Security
    - ECE 579C Applied Cryptography and Physical Attacks
- One human behavior-focused course from:
    - CS 571 Case Studies in Computer Security
    - CS 525 Digital Forensics
    - CS 525 Computer Crime Law
    - ECE 579B Blockchain and Cryptocurrencies
- MIS 582 Information Security Management

MS-SEC students must complete three depth courses from the following:

- ECE 573/CS 578 Cryptography & Data Security
- ECE 673 Advanced Cryptography
- CS 564 Advanced Topics in Computer Security
- OIE 542 Risk Management & Decision Making
- Any core course from above that has not been used to satisfy the core requirement.

In the standard track, our bridge component supports students with less preparation to help them learn core concepts needed in subsequent classes. While highly recommended for those without previous technical preparation related to the field, these courses are optional preparation. Students who already have significant preparation in these areas, through undergraduate classes, graduate classes, or professional experience may choose not to take one or more bridge course without requiring advisor or program approval. For students on the software-centric standard track, CS 5007, CS 5008, and CS 509 are useful preparation.

In the advanced track, students may choose not to take any of the bridge courses and instead focus on technical depth or electives. Students on the advanced software-centric track may prefer to take either CS 557 or CS 558. Students on the advanced hardware-centric track may prefer to take DS/ECE 577 Machine Learning in Cybersecurity or ECE 579C Applied Cryptography and Physical Attacks.

MS-SEC students who do not take all of the bridge courses may select to take thesis credits or additional elective courses from the following to reach the 30-credit requirement:

- CS 502 Operating Systems
- CS 513 Computer Networks

- CS 534 Artificial Intelligence
- CS 539 Machine Learning
- CS 542 Database Management Systems
- CS 546 Human-Computer Interaction
- CS 548 Knowledge Discovery and Data Mining
- CS 573 Data Visualization
- ECE 506 Introduction to Local and Wide Area Networks
- ECE 5307 Wireless Access and Localization
- Undergraduate courses through the BS/MS program that have significant material overlap with the above graduate courses, as specified in the following section.
- Any core or depth course from above that has not been used to satisfy either the core or depth requirements.

MS-SEC students must complete a three-credit capstone project experience or a nine-credit MS Thesis from the following:

- CS 587/ECE 588 Cyber Security Capstone Experience
- CS 599/ECE 599 Master's Thesis

In the core requirements, students are exposed to a technically-oriented course, a human behavioral dimension course, and a course that relates security to business needs. This combination allows students to put technical material into a societal context.

With these requirements, students on the standard track may complete 3 bridge courses, 3 core courses, 3 depth courses, and the capstone experience for a total of 30 credits. Students on the advanced track may omit the bridge courses and instead take 3 core courses, 3 depth courses, 3 elective courses, and the capstone experience totaling 30 credits. For students pursuing a thesis, the capstone and two elective courses may be swapped for a 9-credit MS thesis.

For the Joint Bachelor's/Master's Program

The requirements for the MS-SEC are structured so that undergraduate students would be able to pursue a Bachelor's/Master's program, in which the Bachelor's degree is awarded in any major offered at WPI and the Master's degree is awarded as the MS-SEC. Students enrolled in the joint Bachelor's/Master's program must satisfy all the program requirements of their respective bachelor's degree and all the program requirements of the MS-SEC. WPI allows the double counting of up to 12 credits for students pursuing a 5-year Bachelor’s/Master’s program. This overlap can be achieved through the following mechanisms. Students may double-count courses towards both their undergraduate and graduate degrees whose credit hours total no more than 40 percent of the 30 credit hours required for the MS-SEC, and that meet all other requirements for each degree. These courses can include graduate courses as well as certain undergraduate 4000-level courses as long as the undergraduate courses are acceptable in place of a corresponding graduate course that satisfies a MS-SEC requirement.

In consultation with the academic advisor, the student prepares a Plan of Study outlining the selections chosen to satisfy the Bachelor's/Master's program degree requirements, including the courses that will be double-counted. This Plan of Study must then be approved by the Cyber Security program. As a university wide rule, the B.S./M.S. double counting credits can be applied for only while the student is an undergraduate student.

For the following 4000-level courses, two graduate credits will be earned towards the joint Bachelor's/Master's degree if the student achieves grade B or higher, or otherwise with the instructor's approval. In addition, faculty may offer, at their discretion, an additional 1/6 undergraduate unit, or equivalently a 1 graduate credit, for completing additional work in the course. To obtain this additional credit, the student must register for 1/6 undergraduate unit of independent study at the 4000-level or a 1 graduate credit independent study at the 500-level, with permission from the instructor. A student can receive credit for at most one of the two courses in any row of the following table.

Undergraduate Course	**Graduate Course**
CS 4341 Introduction to Artificial Intelligence	CS 534 Artificial Intelligence
CS 4342 Machine Learning	CS 539 Machine Learning
CS 4401 Software Security Engineering	CS 557 Soft. Security Design & Analysis
CS 4432 Database Systems 2	CS 542 Database Management Systems
CS 4445 Data Mining and Knowledge Discovery in Databases	CS 548 Knowledge Discovery and Data Mining
CS 4513 Distributed Systems	CS 502 Operating Systems
CS 4516 Advanced Computer Networks	CS 513 Computer Networks

Students may additionally double-count CS 4404 (Tools and Techniques in Computer Network Security) or CS 4801/ECE 4802 (Introduction to Cryptography and Communication Security) towards the joint Bachelor's/Master's degree.

Other 4000-level courses not listed above, including 4000-level independent study courses, require a petition and approval from the Cyber Security Graduate Committee before they can double-count for the Bachelor's/Master's degree.

Satisfying MS-SEC Core Areas

Students with Bachelor's/Master's credit for CS 4401 (Software Security Engineering), CS 4404 (Tools and Techniques in Computer Network Security), or CS 4801/ECE 4802 (Introduction to Cryptography and Communication Security) may use that course to satisfy the technically-focused core course requirement. Alternatively, the student may instead apply that course credit

towards either the depth or the elective requirements. For any other undergraduate course or independent study/project work, students may submit a petition along with a detailed course description and syllabus to the Cyber Security Program for final decision on whether the course should count towards core area requirements.