

Master of Science in Cybersecurity

For more information contact:

Sumita Mishra (Sumita.mishra@rit.edu)
Graduate Program Director
Department of Cybersecurity
Global Cybersecurity Institute
Rochester Institute of Technology
100 Lomb Memorial Drive
Rochester, NY 14623-5603
(585) 475-2963 (voice)
(585) 475-2181 (fax)

ROCHESTER INSTITUTE OF TECHNOLOGY
Department of Cybersecurity

Master of Science
in
Cybersecurity

Introduction

The Master of Science in Cybersecurity (CSEC) focuses on the theoretical, organizational, and applied aspects of computing security. The curriculum is unique as it provides both research and applied experiences to our students.

Program Goals and Objectives

Upon completion of the MS in CSEC program, successful students will have acquired the necessary skills to do the following:

- Protect computer systems from the threats, exposures and risks caused by unauthorized access in today's networked computer environment.
- Outline and apply appropriate methods and mechanisms that can be used to protect enterprise data to help manage the risk of unauthorized data access, data tampering, or theft.
- Communicate effectively, both orally and in writing, with other security and computing professionals.
- Research security issues, synthesize the information, and communicate the results of the research to business and computing professionals.
- Design and analyze basic cryptographic algorithms and protocols.
- Apply appropriate software engineering techniques to address security needs in software development.
- Evaluate security mechanisms in terms of their effectiveness, maintenance and appropriateness in computer networks.
- Evaluate ethical controversies and use various decision-making approaches for resolving ethical dilemmas in complex situations.

Program Design

The MS in Cybersecurity program consists of two (2) core courses and two (2) research electives that provide a knowledgebase in the theoretical principles and advances in computing security and information assurance today. Together, these courses ensure that graduates acquire the intellectual tools necessary to stay up-to-date in this challenging and rapidly evolving discipline. Students can then develop depth in an area of expertise in systems and network security, systems and network forensics, secure coding, and security theory by selecting four or five related elective courses. The program of study is capped off with one of the following: a six-credit thesis, a three-credit project, or a three-credit capstone course.

This MS degree comprises 30 semester-credits of graduate study which include:

- 2 core courses (6 credits); focusing on foundation of computer security concepts and cryptography
- 2 research electives (6 credits): focusing on research areas in cybersecurity
- 5 or 6 elective courses (12 - 15 credits), depending upon the capstone option chosen, to develop breadth and depth in security topics of individual interest
- MS capstone experience: a thesis (6 credits), a project (3 credits), or a capstone course (3 credits)

Entrance Requirements

MS in Cybersecurity is designed for individuals whose undergraduate degree is in a computing discipline with a solid theoretical foundation in computing and mathematics (such as Computer Science, Computer Engineering or related fields). Exceptional students from other disciplines may be admitted with the

contingency of completing a bridge study as assigned by the graduate program director and the faculty, to ensure that they have the prerequisite knowledge necessary for success in this program.

Degree applicants should minimally have a baccalaureate or equivalent degree from an accredited institution of higher education and a minimum cumulative grade-point average equivalent to 3.0/4.0 ('B' average). International students must also have equivalent of at least a 3.0/4.0 from an accredited university using the US system of grading or at least a first-class degree from an accredited university using the British system of grading. Additionally, applicants with degrees from foreign universities must submit Graduate Record Examination (GRE) scores¹.

Applicants whose native language is not English must take and submit the TOEFL examination. A minimum score of 570 (paper-based exam) or 88 (internet-based exam) is required (Note that students with TOEFL scores between 88 and 96 are admitted conditionally but have to go through additional testing offered through English Language Center at RIT. They might be required to take a prescribed program in English along with a reduced program course load until the required English level is achieved).

Information about the GRE and the TOEFL examinations is available at <http://www.ets.org>.

Prerequisites

- Competency in Discrete Mathematics and Statistics (Calculus recommended)
- Solid skills in computer programming (proficiency in two programming languages required)
- Knowledge and hands-on experience in basic networking concepts, including: Ethernet, TCP/IP, routing and switching, and basic LAN design and construction principles.
- Knowledge of basic networking infrastructure services, including DHCP, DNS, and other discovery and name resolution protocols.
- Knowledge of basic system services and system administration functions, including scripting for UNIX, user administration, networked file systems, web services, networked information systems (such as NIS), and networked security and permission issues.

The Bridge Program

All students must have the required coursework and documented experience before matriculating into the COMPSEC MS program. Students, whose undergraduate preparation or industrial/work experience does not satisfy the above requirements can make up this deficiency by taking one or more courses as prescribed by the graduate program director and faculty. This coursework may be completed at any accredited college or university.

The courses offered by RIT that can be used to satisfy the above prerequisites are:

- Discrete mathematics (equivalent to MATH 190 Discrete Mathematics for Computing)
- Statistics (equivalent to STAT-145 or MATH-251)
- Computer Programming skills (equivalent to CSCI-141 Intro to Programming I and CSCI-142 Intro to Programming II or GCIS-123 Software Development & Problem Solving I and GCIS-124 Software Development & Problem Solving II)
- Introduction to Computing Security (CSEC-600)

Students are expected to achieve a 3.0 ('B' grade) or better average in course work done as part of the bridge program. Bridge program courses are not part of the 30-semester credit hours required for the master's degree. Grades for bridge courses taken after matriculation are included in student's graduate grade-point average.

Students who have been admitted to the program before completing prerequisite requirements must satisfactorily complete bridge coursework within the first two semesters of matriculation to continue in the

¹ RIT's reporting number for ETS's GRE and TOEFL examinations is 2760.

program. Prior approval of the graduate program director is required before any other courses in the program may be taken.

To meet individual needs, a bridge program can be designed differently from that described above. Other courses can be substituted, or courses at other colleges can be applied. **However, such courses must be approved in advance.** Contact the graduate program director (see contact information later in this document) for approval prior to beginning bridge coursework.

Application & Deadlines

Please refer to <https://www.rit.edu/admissions/graduate#applying-for-admission> for instructions and requirements of the application. Student applications are considered for **Fall term only**. We have no specific deadlines and applications are processed on a rolling basis, until the program reaches its capacity for the academic year. The application process typically takes four to six weeks after the Office of Graduate Enrollment Services (GES) has received a complete application. However, international applications may take longer. The graduate program director only evaluates applications after all of the information has been submitted and verified by staff in the RIT office of graduate admissions.

Note that acceptance into the program does not guarantee availability of prerequisite or program courses. As the start of the semester approaches, many classes become full. Students who apply just before the start of the year, may need to wait until the following year, before starting their coursework.

Full time course load

MS students are enrolled in at least 9 credits of coursework per semester to be considered full time. International students seeking an I-20 to reside in the United States while studying in this program should note that they are required to be enrolled for at least nine (9) credits per semester to maintain their full-time status. Of those 9 credits, international students may **only count one (1)** online course (or 3 credits) towards their full-time course load. They may take additional online courses “outside” of the 9 credits.

The Curriculum (MS in CSEC)

Core Classes (6 credits)

- GCCIS-CSEC-604 Cryptography and Authentication
- GCCIS-CSEC-742 Computer System Security

Research Electives (6 credits)

- GCCIS-CSEC-659 Graduate Seminar on Usable Security and Privacy
- GCCIS-CSEC-720 Deep Learning Security
- GCCIS-CSEC-741 Internet of Things Security
- GCCIS-CSEC-750 Covert Communications
- GCCIS-CSEC-759 Graduate Seminar on Advanced Networking and Distributed Systems Security
- GCCIS-CSEC-759 Graduate Seminar on Advanced Malware Forensics
- GCCIS-CSEC-759 Graduate Seminar on Internet Security
- GCCIS-CSEC-759 Graduate Seminar on Human Factors
- GCCIS-CSEC-769 Emerging Topics in Wireless Security

Advanced Electives (12 or 15 credits)

- GCCIS-CSEC-603 Enterprise Security
- GCCIS-CSEC-620 Cyber Analytics and Machine Learning
- GCCIS-CSEC-630 Trusted Computing
- GCCIS-CSEC-659 Graduate Seminar on Hacking for Defense
- GCCIS-CSEC-659 Graduate Seminar on Offensive Security Engineering
- GCCIS-CSEC-659 Graduate Seminar on Blockchains and Smart Contracts
- GCCIS-CSEC-669 Wireless Security
- GCCIS-CSEC-730 Advanced Computer Forensics
- GCCIS-CSEC-731 Web Server and Application Security Audits
- GCCIS-CSEC-733 Information Security and Risk Management
- GCCIS-CSEC-743 Computer Viruses and Malicious Software
- GCCIS-CSEC-744 Network Security
- GCCIS-CSEC-751 Information Security Policy and Law
- GCCIS-ISTE-721 Information Assurance Fundamentals
- GCCIS-ISTE-730 Foundations of IoT
- GCCIS-CSCI-620 Introduction to Big Data
- GCCIS-CSCI-622 Data Security and Privacy
- GCCIS-CSCI-635 Introduction to Machine Learning
- GCCIS-CSCI-642 Secure Coding
- GCCIS-CSCI-655 Foundations of Cybersecurity
- GCCIS-CSCI-662 Foundations of Cryptography
- GCCIS-CSCI-720 Big Data Analytics
- GCCIS-CSCI-735 Foundations of Intelligent Security Systems
- GCCIS-CSCI-762 Advanced Cryptography
- KGCoe-CMPE-661 Hardware and Software Design for Cryptographic Applications

CSEC Capstone (3 or 6 credits)

- GCCIS-CSEC-790 MS Thesis (6 credits) or
- GCCIS-CSEC-792 CSEC Project (3 credits) or
- GCCIS-CSEC-793 Capstone for Computing Security (3 credits)

Course plan for MS in Cybersecurity

CORE COURSES (6 credits)	
CSEC 604 Cryptography and Authentication	CSEC 742 Computer System Security

RESEARCH ELECTIVES (choose 6 credits)				
CSEC 720 Deep Learning Security	CSEC 741 Internet of Things Security	CSEC 750 Covert Communications	CSEC 769 Emerging Topics in Wireless Security	CSEC 659/759 <i>Has to be a research seminar (see page 5)</i>

ADVANCED ELECTIVES IN SUGGESTED AREAS (choose 12 to 15 credits)			
Systems and Network Security	Systems and Network Forensics	Cryptography and Authentication	Cyber Analytics
*CSEC-603 Enterprise Security	*CSEC-730 Advanced Computer Forensics	*CSCI-662 Foundations of Cryptography	*CSEC-620 Cyber Analytics and Machine Learning
*CSEC-744 Network Security	*CSEC-731 Web Server and Application Security Audits	*CSCI-762 Advanced Cryptography	*CSEC-720 Deep Learning Security
CSEC-659 Seminar on Offensive Security Engineering	CSEC-732 Mobile Device Forensics	CSCI-734 Foundations Of Security Measurement and Evaluation	CSEC-730 Advanced Computer Forensics
CSEC-669 Wireless Security	CSEC-733 Information Security and Risk Management	CSCI-735 Foundations of Intelligent Security Systems	CSCI-620 Introduction to Big Data
CSEC-733 Information Security and Risk Management	CSEC-743 Computer Viruses and Malicious Software	CMPE-661 Hardware and Software Design for Cryptographic Applications	CSCI-622 Data Security and Privacy
			CSCI –635 Introduction to Machine Learning

Note: *means strongly suggested for students studying in the corresponding areas of focus

Note 2: Several research/advanced elective seminars are available in each area of focus. Please consult the graduate program director for recommendations for a particular area.

CAPSTONE (3 or 6 credits)		
CSEC-790 MS Thesis (6 credits)	CSEC-791 MS Project (3 credits)	CSEC-793 MS Capstone Class (3 credits)

Graduate Independent Study

Graduate students may undertake up to **one (1) Independent Study** (3 credits) to investigate a cybersecurity area that is of interest. This independent study may replace one of the advanced electives (NOT a research elective). The emphasis of independent study is that it is driven by a student's interest in investigating an area in a way that cannot be done through standard course work. It may or may not be connected with a faculty member's scholarship activities, but it does require a faculty member to approve the work as the advisor for the independent study, as well as the approval from the department.

Students will follow a structured application process prior to registering for Independent Study. Please ask your sponsoring faculty member for the form. Once completed, the form needs to be submitted to the department by the sponsoring faculty member. At the conclusion of the independent study, the student will make a formal presentation to the department faculty, describing the results of the work undertaken.

Co-operative Work Experience

Up to two (2) terms of an *optional* co-operative educational experience (co-op) is available, prior to capstone completion, for those students who wish to enhance their resume with employment experience. Students need to complete all bridge study (including English Language Center study), have completed 15 credits of their MS course work, and have a 3.0/4.0 or better program grade-point-average (GPA) before going on co-op. Students on academic probation are ineligible to go on a co-op.

The Office of Cooperative Education and Career Services (<http://www.rit.edu/emcs/oce/>) can assist students in finding a co-op position or students can find positions on their own and have them approved by the graduate program director.

Program Cost

The cost of graduate study at RIT is available on the RIT website at (<https://www.rit.edu/admissions/tuition-and-fees>). Cost information is available for both full- and part-time study. Information about financial aid to support study with us is available at <https://www.rit.edu/admissions/financial-aid>

Financial Aid

The department can offer a small Merit Scholarship to qualified students who are not receiving significant financial support from other sources. This award is based upon previous educational performance, and employment background (if applicable). If granted, the merit scholarship is initially awarded for one (1) academic year from the semester in which the student is admitted. The award will, in general, be extended if the student has made steady progress towards the degree and has maintained at least a 3.0/4.0 GPA, which is the minimum required to graduate with a MS degree at RIT.

RIT's 7-Year Degree-Completion Rule

Graduate students must successfully complete all of the requirements for their programs within seven (7) years of the date of the first (oldest) course counted towards the degree. This requirement includes courses transferred into the program from other RIT departments or other universities, but excludes prerequisite courses. For example, if the first course was completed in Fall term 2023 (2231), then the program must be completed before the start of Fall term 2030 (2301). Please contact the graduate program director immediately if you find that you are coming close to your 7-year deadline.

Academic Honesty

Academic honesty is an expectation of all students at RIT. Any act of improperly representing another person's work as one's own is an act of academic dishonesty. The RIT code of academic conduct is documented in the university's Policies and Procedures manual:

<https://www.rit.edu/academicaffairs/policiesmanual/d080>

RIT Non-Discrimination Statement

RIT does not discriminate. RIT promotes and values diversity within its workforce and provides equal opportunity to all qualified individuals regardless of race, color, creed, age, marital status, sex, gender, religion, sexual orientation, gender identity, gender expression, national origin, veteran status, or disability.

Contact Information

Additional information about this program and other programs offered by the Cybersecurity (CSEC) department at RIT may be obtained by contacting us at:

US Mail: Graduate Program Director
Department of Cybersecurity
Global Cybersecurity Institute
Rochester Institute of Technology
100 Lomb Memorial Drive
Rochester, New York 14623-5603

Telephone: (585) 475-2963

FAX: (585) 475-2181

Academic Calendar

RIT academic calendar is available at www.rit.edu/calendar/.

MS in CSEC Program Worksheet (as of 2023 -2024)

PAGE 1

<i>Prerequisite Bridge Program ¹</i>		Must be completed prior to start of program of study.	
Programming I			
Programming II			
Discrete Mathematics			
Statistics			
CSEC 600 – Introduction to Computing Security			
~ Program of Study (30 semester credit hours) ~			
Core Courses: (6 credit hours)	Semester	Grade	Comments
GCCIS-CSEC-742 Computer Systems Security			
GCCIS-CSEC-604 Cryptography and Authentication			
Research Electives: (6 credit hours) ²			
Advanced Electives: (12 – 15 credit hours) ²			
Capstone: (3 or 6 credit hours) ³			
CSEC-79__ Capstone [Course Project]			(3 credits)
CSEC-790 Thesis			(6 credits)

WORKSHEET (PAGE 2)

Completion of Program of Study:

To earn the MS degree, you must complete the prerequisites/bridge and degree requirements shown on the previous page. Contact your academic advisor periodically to review your progress and receive an updated copy.

Good Academic Standing

A 3.0 GPA or higher is required to graduate. All courses (undergraduate or graduate) taken after matriculating into an MS program at RIT are counted towards your grade-point average (GPA). To be in good academic standing, a graduate student at RIT must maintain a cumulative GPA of 3.0/4.0 or better throughout a program of study. RIT institute policy states that 'C-', 'D' or 'F' grades do not count toward the fulfillment of program requirements for a graduate degree." *However, they are calculated into your GPA.*

Discontinued Status

After three (3) consecutive terms without registration activity (summer term counts), the RIT Registrar will change your status to "de-matriculated," which means that you are no longer a student in the MS/CSEC program. To return to matriculated status, you will need to reapply to RIT. If more than two years have elapsed since you were matriculated, your program of study will be reviewed, and you may have to complete the degree requirements currently in effect to obtain your degree. This could mean loss of waivers and transfer credit as well as doing additional coursework for readmission or degree completion.

Course Waivers

On rare occasions, a required course may be waived due to prior academic or employment experience. If this occurs, to complete the total number of credits required for the degree, the student must take another course to replace the one that was waived. This does not apply to prerequisite courses.

Bridge Courses

Bridge/Prerequisite courses must be completed within the first two terms after matriculation.

Research Electives

Students in the MS/CSEC program must complete two (2) Research Electives. Students may select between the following courses to complete this requirement: CSEC 720, CSEC 741, CSEC 750 and CSEC 769. In addition to these courses, the department offers a few seminar courses that count as research electives. Seminar course fall under CSEC 659 and CSEC 759, **however not all seminars are research electives.**

Advanced Electives

Advanced Electives should be chosen in consultation with your graduate faculty and graduate academic advisor. Ideally, these courses should be selected to focus on one specific area, or at most two synergistic areas of interest. Certain electives may require additional prerequisite study. One less elective is needed with a thesis capstone.

MS Capstone

Students in the MS/CSEC program can choose between three different capstone options: Project (3cr), Course (3cr), or Thesis (6cr). If a student chooses to pursue the thesis option, they will complete one less advanced elective. For more information about capstone requirements and the difference between the three options please see the capstone guide located under the MS Student Resources: <https://www.rit.edu/computing/departments-computing-security/resources>. To enroll in MS Capstone, you must have an approved project proposal prior to enrollment. The proposal should be developed during the term prior to the intended enrollment term. The last date to submit your signed/approved proposal to the department office and the graduate program director is the first day of classes of the intended enrollment term.

Co-op Enrollment

While co-op is not a requirement for students in the MS/CSEC program, many of our students chose to pursue a coop during their MS career. To be eligible for a co-op, a student must have completed all prerequisite classes and 15 credits of MS coursework. Additionally, students must receive approval from the Graduate Director prior to reporting a co-op. When seeking approval, the student must submit the job offer to the Graduate Director via email. If approved, the student must then report the co-op through RIT's Co-op office's website. Once reviewed by their office, the CSEC department will enroll you in SIS. You cannot enroll in Co-op in SIS yourself.