RIT | Department of Cybersecurity

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 three (3) core courses, two (2) research electives, and three (3) advanced electives that provide a knowledge base in the theoretical and practical principles of 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 develop depth in an area of expertise in systems and network security, systems and network forensics, cryptography and authentication, and cyber analytics. The program of study is capped off with one of the following: a six-credit thesis, or an additional (research elective + advanced elective).

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

- 3 core courses (9 credits): focusing on the foundation of computer security concepts, cryptography, and enterprise security.
- 2 research electives (6 credits): focusing on research areas in cybersecurity.
- 3 advanced elective courses (9 credits): to develop breadth and depth in security topics of individual interest.
- MS capstone experience/exit strategy (6 credits): Option 1: MS Thesis (6 credits), or Option 2: an additional research elective (3 credits) + advanced elective (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 an 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) scores[1]

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 must go through additional testing offered through the 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, including Python, 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 does not satisfy the above requirements can make up for this deficiency by taking one or more courses as prescribed by the graduate program director and faculty. This coursework may be completed at RIT or 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 coursework 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 the 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 program. Prior approval of the graduate program director is required before any other courses in the program may be taken.

---

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

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 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 the 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 (9 credits)
- GCCIS-CSEC-604 Cryptography and Authentication
- GCCIS-CSEC-742 Computer System Security
- GCCIS-CSEC-603 Enterprise Security*

Research Electives (6 credits)
- GCCIS-CSEC-720 Deep Learning Security
- GCCIS-CSEC-741 Internet of Things Security
- GCCIS-CSEC-750 Covert Communications
- GCCIS-CSEC-759 Graduate Seminar in Advanced Networking and Distributed Systems Security
- GCCIS-CSEC-759 Graduate Seminar in Advanced Malware Forensics
- GCCIS-CSEC-759 Graduate Seminar in Advanced Software Security
- GCCIS-CSEC-759 Graduate Seminar in Human Factors in Security
- GCCIS-CSEC-769 Emerging Topics in Wireless Security

Advanced Electives (9 credits)

• GCCIS-CSEC-620 Cyber Analytics and Machine Learning • GCCIS-CSEC-622 Side Channel Analysis • GCCIS-CSEC-630 Trusted Computing and Trusted Execution • GCCIS-CSEC-635 Open-Source Software Security • GCCIS-CSEC-659 Graduate Seminar in Offensive Security Engineering • GCCIS-CSEC-659 Graduate Seminar in Blockchains and Smart Contracts • GCCIS-CSEC-659 Graduate Seminar in Open-Source Intelligence • GCCIS-CSEC-659 Graduate Seminar in Generative AI in Cybersecurity • GCCIS-CSEC-659 Seminar in Social Engineering • GCCIS-CSEC-669 Wireless Security • GCCIS-CSEC-677 Disaster Recovery • 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-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-764 Quantum-Resistant Cryptography • KGCOE-CMPE-661 Hardware and Software Design for Cryptographic Applications

*CSEC-603 is a new core class required for all MS students beginning in Fall 2025 and after and all BSMS students with their Requirement Term as 2251 and beyond. For everyone else, it is an advanced elective.

**Students taking CSCI-662 need a replacement class for CSEC-604 due to overlapping content.

CSEC Capstone/Exit Strategy (6 credits)
- GCCIS-CSEC-790 MS Thesis (6 credits) or
- An additional research elective (3 credits) + an advanced elective (3 credits) from the lists above

Course plan for MS in Cybersecurity

CORE CLASSES (9 credits)

CSEC 603^ Enterprise Security	CSEC 604 Cryptography and Authentication	CSEC 742 Computer Systems 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 759 *Must be a research seminar (see page 5)*

ADVANCED ELECTIVES IN SUGGESTED AREAS (choose 9 credits)

Systems and Network Security	Systems and Network Forensics	Cryptography and Authentication	Cyber Analytics
*CSEC-744 Network Security *CSEC-659 Seminar on Offensive Security Engineering CSEC-669 Wireless Security CSEC-733 Information Security and Risk Management	*CSEC-730 Advanced Computer Forensics *CSEC-731 Web Server and Application Security Audits CSEC-732 Mobile Device Forensics CSEC-733 Information Security and Risk Management CSEC-743 Computer Viruses and Malicious Software	*CSEC-659 Graduate Seminar in Blockchains and Smart Contracts *CSCI-764 Quantum Resistant Cryptography CSEC-630 Trusted Computing and Trusted Execution CSCI-622 Data Security and Privacy CMPE-661 Hardware and Software Design for Cryptographic Applications	*CSEC-620 Cyber Analytics and Machine Learning *CSEC-659 Graduate Seminar in Generative AI in Cybersecurity CSEC-730 Advanced Computer Forensics CSCI-720 Big Data Analytics CSCI-735 Foundations of Intelligent Security Systems

^Please see the note on CSEC603 on page 5

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/EXIT STRATEGY (6 credits)
(pick one option)

CSEC-790 MS Thesis (6 credits)	MS Research Elective (3 credits) + MS Advanced Elective (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 coursework. It may or may not relate to 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 approval from the department.

Students will follow a structured application process before 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. Co-ops are not required for obtaining the MS degree, but are highly encouraged. 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 may 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 an MS degree at RIT.

RIT's 7-Year Degree-Completion Rule

Graduate students must complete all of the requirements for their programs within seven (7) years of the date of the student's matriculation into the program. https://www.rit.edu/policies/d120#vii-seven-year-graduation-requirement For example, if the student was matriculated in the program in Fall term 2025 (2251), then the program must be completed before the start of Fall term 2032 (2321). 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