COMPUTING SECURITY

Master of Science
in
Computing Security

For more information contact:

Rochester Institute of Technology
Department of Computing Security
152 Lomb Memorial Drive
GOL-2120
Rochester, NY 14623-5603
(585) 475-2963 (voice)
(585) 475-2184 (fax

ROCHESTER INSTITUTE OF TECHNOLOGY
Department of Computing Security

Master of Science
in
Computing Security

Introduction

In recent years, there have been ever increasing numbers of computer-based crimes against the information and economic infrastructure of our society. A number of troubling trends have emerged: the time from the discovery of a vulnerability to the creation of its exploit has shortened dramatically; attackers are increasingly focusing on attacks that cause the most harm to public and private networks; confidential data is increasingly becoming the focus of attacks in support of criminal activity; and attackers are developing large, highly sophisticated networks of "compromised" computers for denial-of-service and other cyber attacks. However, despite these risks, organizations of all shapes and sizes are establishing "web identities" and looking to computing technologies and interconnectivity to enhance both their employee productivity and competitiveness in the face of global competition. These trends have lead to additional responsibilities for network and system administrators along with the emergence of a new computing specialization, that of the computer security specialist.

The Master of Science in Computing Security (MS/CSEC) focuses on the theoretical, organizational, and applied aspects of computing security. The curriculum is unique in its recognition of the need for students to have a broad-based understanding of the myriad of issues involved in providing secure, yet useful, computing environments that enhance the productivity of users while at the same time living up to the fundamental pillars of computing security as enhanced to encompass the full scope of information assurance: confidentiality, integrity, availability (together, the CIA principle), plus authentication and non-repudiation.

Program Goals and Objectives

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

- Protect computer systems from the threats, exposures and risks, possible through 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 Computing Security program consists of two (2) core courses and two (2) research electives that provide a common knowledge-base in the theoretical principles underlying 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 a six-credit thesis, a three-credit project, or a three-credit capstone course.

The program includes courses that enable students to understand the theoretical foundations of computing security, to join a team of professionals solving the challenges of ensuring secure computing environments, and to become leaders in implementing solutions computing security and information assurance. Alternately, students can prepare for further academic study and careers in academia or research.

MS in Computing Security is designed for individuals whose undergraduate major, or minor, was in a computing discipline with a solid theoretical foundation as well as those who have a strong background in a field to which computers are applied, such as Engineering, Science, or Mathematics. Students admitted without this background must complete bridge study as assigned by the Graduate Director and the faculty to ensure that they have the prerequisite knowledge necessary for success in this program.

This MS degree is comprised of 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)

A wide variety of support services are available including advising, online library catalogs and indexes (some with full text), inter-library loans, internet-based audio conferences, computer conferencing, etc.

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 1** online course (or 3 credits) towards their full-time course load. They may take additional online courses "outside" of the 9 credits.

Entrance Requirements

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) scores[1]. The GRE may also be required for those applicants requesting consideration whose undergraduate grade-point average is less than 3.0/4.0.

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). Other evidence of language proficiency, such as writing samples and GRE scores, may also be evaluated to assess functional English ability.

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

Application & Deadlines

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 director only evaluates applications after all of the information has been submitted and verified by staff in the RIT office of graduate admissions. Please refer to https://www.rit.edu/emcs/ptgrad/grad_admission.php for instructions and requirements of the application.

Student applications are considered for Fall term admission only. However, 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 course work.

Prerequisites

Applicants wishing to enter this master's program should have an undergraduate degree in computing related areas with a solid education in mathematics, statistics and computer programming fundamentals. Programs that may provide the necessary background are degrees in Computing Security, Computer Science, Software Engineering, Computer Engineering – depending upon the student's previous course work and/or work experience. The specific prerequisites are:

- Mathematical maturity, including Integral and Differential Calculus and Discrete Mathematics.
- Statistics
- Solid skills in computer programming.
- Knowledge in natural sciences such as physics, biology, etc.
- 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.

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

The Bridge Program

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

The courses offered by RIT that can be used to satisfy the above prerequisites are (prerequisites and notes are included in parentheses after each course):

- 2-course Calculus sequence (equivalent to COS-MATH 181 Project-Based Calculus I and COS-MATH 182 Project-Based Calculus II)
- Discrete mathematics (equivalent to COS-MATH 190 Discrete Mathematics for Computing)
- Computer Programming skills (equivalent to CSCI-141 Intro to Programming I and CSCI-142 Intro to Programming II and CSCI-242 Mechanics of Programming)
- Statistics (equivalent to STAT-145 or MATH-251)
- Introduction to Computing Security (CSEC 600) OR (Computer Networking (equivalent to NSSA-606) AND Systems Administration (equivalent to NSSA-605))

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. Bridge courses may not be applied towards degree requirements. If taken before matriculation, grades for bridge courses are not included in a student's graduate grade-point average. However, 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 program. Prior approval of the graduate 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 director (see contact information later in this document) for approval prior to beginning bridge coursework.

The Curriculum

MS/CSEC Core (6 credits)

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

Research Electives (6 credits)

- GCCIS-CSEC-741 Sensor and SCADA Security
- GCCIS-CSEC-750 Covert Communications
- GCCIS-CSEC-759 Graduate Seminar in Computing Security – Wireless Security
- GCCIS-CSEC-759 Graduate Seminar in Computing Security – Advanced Malware Forensics and Anti-Forensics
- GCCIS-CSEC-759 Graduate Seminar in Computing Security – Internet Security and Privacy

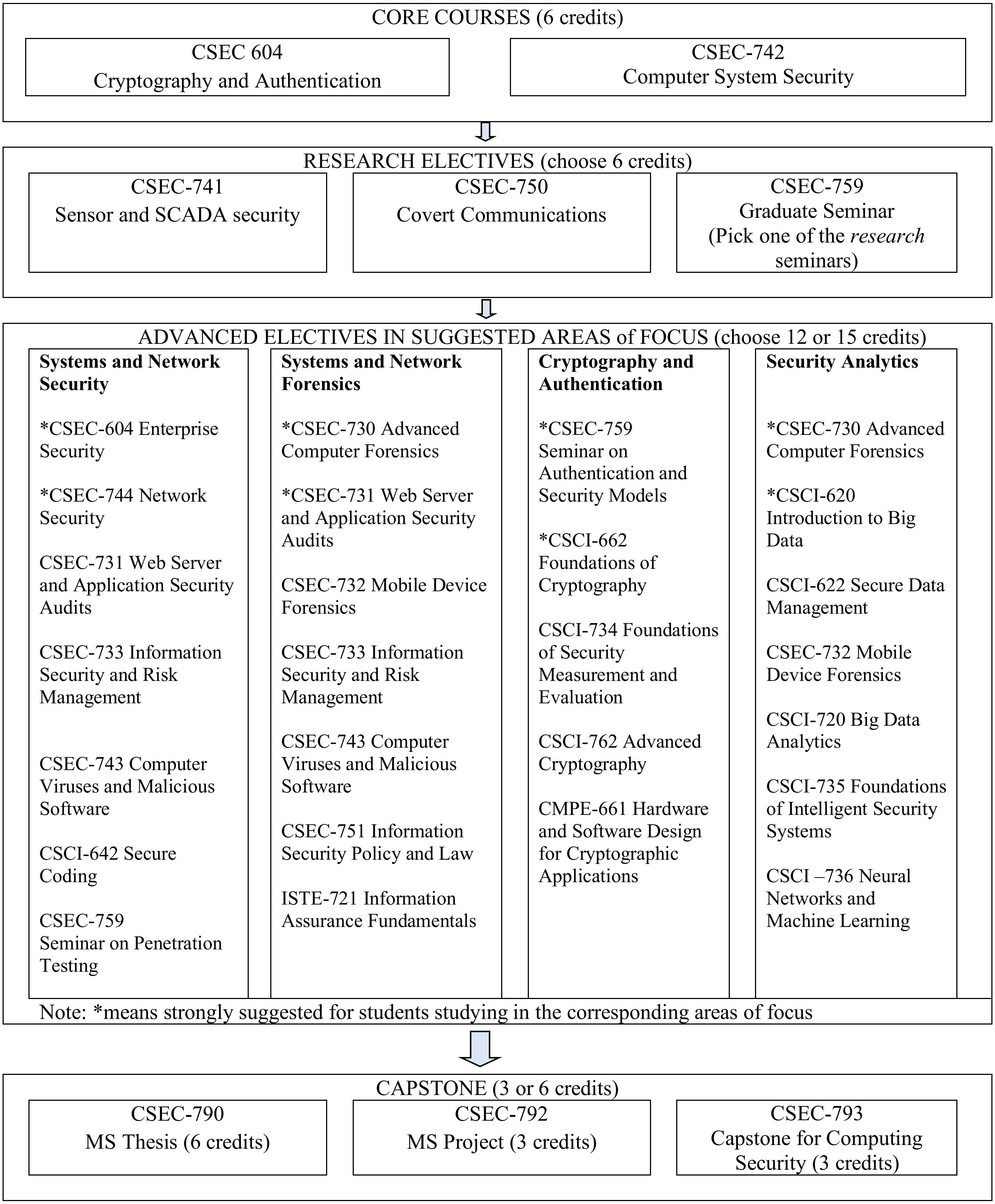
Advanced Electives (12 or 15 credits)

- GCCIS-CSEC-603 Enterprise Security
- GCCIS-CSEC-730 Advanced Computer Forensics
- GCCIS-CSEC-731 Web Server and Application Security Audits
- GCCIS-CSEC-732 Mobile Device Forensics
- GCCIS-CSEC-733 Information Security and Risk Management
- GCCIS-CSEC-741 Sensor and SCADA Security
- GCCIS-CSEC-743 Computer Viruses and Malicious Software
- GCCIS-CSEC-744 Network Security
- GCCIS-CSEC-750 Covert Communications
- GCCIS-CSEC-751 Information Security Policy and Law
- GCCIS-CSEC-759 Graduate Seminar on Wireless Security
- GCCIS-CSEC-759 Graduate Seminar on Advanced Malware Forensics
- GCCIS-CSEC-759 Graduate Seminar on Penetration Testing
- GCCIS-CSEC-759 Graduate Seminar on Internet Security and Privacy
- GCCIS-ISTE-721 Information Assurance Fundamentals
- GCCIS-CSCI-620 Introduction to Big Data
- GCCIS-CSCI-622 Secure Data Management
- GCCIS-CSCI-642 Secure Coding
- GCCIS-CSCI-662 Foundations of Cryptography
- GCCIS-CSCI-720 Big Data Analytics
- GCCIS-CSCI-734 Foundations of Security Measurement and Evaluation
- GCCIS-CSCI-735 Foundations of Intelligent Security Systems
- GCCIS-CSCI-736 Neural Networks and Machine Learning
- GCCIS-CSCI-762 Advanced Cryptography
- KGCOE-CMPE-661 Hardware and Software Design for Cryptographic Applications

The MS/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)

Details of the MS Capstone options can be found in the MS CSEC Capstone Guide posted on the department website.



CORE COURSES (6 credits)

CSEC 604
Cryptography and Authentication

CSEC-742
Computer System Security

RESEARCH ELECTIVES (choose 6 credits)

CSEC-741
Sensor and SCADA security

CSEC-750
Covert Communications

CSEC-759
Graduate Seminar
(Pick one of the *research* seminars)

ADVANCED ELECTIVES IN SUGGESTED AREAS of FOCUS (choose 12 or 15 credits)

Systems and Network Security

*CSEC-604 Enterprise Security

*CSEC-744 Network Security

CSEC-731 Web Server and Application Security Audits

CSEC-733 Information Security and Risk Management

CSEC-743 Computer Viruses and Malicious Software

CSCI-642 Secure Coding

CSEC-759
Seminar on Penetration Testing

Systems and Network Forensics

*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-751 Information Security Policy and Law

ISTE-721 Information Assurance Fundamentals

Cryptography and Authentication

*CSEC-759
Seminar on Authentication and Security Models

*CSCI-662
Foundations of Cryptography

CSCI-734 Foundations of Security Measurement and Evaluation

CSCI-762 Advanced Cryptography

CMPE-661 Hardware and Software Design for Cryptographic Applications

Security Analytics

*CSEC-730 Advanced Computer Forensics

*CSCI-620
Introduction to Big Data

CSCI-622 Secure Data Management

CSEC-732 Mobile Device Forensics

CSCI-720 Big Data Analytics

CSCI-735 Foundations of Intelligent Security Systems

CSCI –736 Neural Networks and Machine Learning

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

CAPSTONE (3 or 6 credits)

CSEC-790
MS Thesis (6 credits)

CSEC-792
MS Project (3 credits)

CSEC-793
Capstone for Computing Security (3 credits)

Figure 1: Course plan for MS in Computing Security

Graduate Independent Study

Graduate students may undertake up to 2 independent study projects (3 credits each) to investigate a cybersecurity area that is of interest. 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 project work as the advisor for the project, as well as the approval from the department.

Students will follow a structured application process prior to registering for Independent Study. Please refer to the "Independent Study form" under "Graduate Forms" for the required details. Once completed, the form needs to be submitted to the department by the sponsoring faculty member. At the conclusion of the project, the student will make a formal presentation to the department faculty, describing the results of the project.

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 course work, and have a 3.0/4.0 or better program grade-point-average (GPA) before going on 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 director.

Program Cost

The cost of graduate study at RIT is available on the RIT website at https://www.rit.edu/fa/sfs/billing-information. Cost information is available for both full- and part-time study. Information about financial aid to support study with us is available at www.rit.edu/emcs/financialaid/graduate.html

Departmental Financial Aid

The CSEC 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 demonstrated need, previous educational performance, and employment background (if applicable).

If granted, the merit scholarship is initially awarded for one (1) academic year (excluding summer) from the semester in which the student is admitted. For the summer term, the student must request continuation of the scholarship. 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.

The Computing Security department offers a limited number of graduate assistantship (GA) positions to individuals with strong academic, interpersonal and technical skills for the purpose of supporting the educational and research activities of the department. These positions can also provide financial support for the qualifying students in the department. Assistantships are awarded for a maximum of one (1) academic year. Both full and part-time assistantships may be offered. A full-time assistantship provides up to full tuition benefits plus an hourly wage each academic term; a part-time assistantship covers a portion of the cost of tuition and an hourly wage. The student is responsible for all degree-related financial obligations not covered by the award.

A full-time GA works 20 hours per week for the department; part time GA works 10 hours per week. Graduate assistants are not responsible for direct course delivery. Instead they may be teaching assistants, or tutors in the undergraduate program, support the faculty in their research efforts or support the Systems Administrator with the lab infrastructure. A GA must maintain good academic standing (U≥U 3.3/4.0 GPA; ethical behavior) to retain the assistantship. An assistantship may be terminated at any time due to unacceptable performance or unethical behavior.

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 2017 (2171), then the program must be completed before the start of Fall term 2024 (2241). Please contact the graduate 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

Contact Information

Additional information about this program and the undergraduate program offered by the Computing Security (CSEC) department at RIT may be obtained by contacting us at:

US Mail: Graduate Program Director
Computing Security Department
Golisano College of Computing & Information Sciences
Rochester Institute of Technology
152 Lomb Memorial Drive
Rochester, New York 14623-5603

Telephone: (585) 475-2963

FAX: (585) 475-2181

Course Descriptions

Courses descriptions are available at https://mycampus.rit.edu/psc/sasrch/EMPLOYEE/HRMS/c/COMMUNITY_ACCESS.SSS_BROWSE_CATLG.GBL - Choose CSEC.

Information about course availability is also available on the RIT website at https://mycampus.rit.edu/psc/sasrch/EMPLOYEE/HRMS/c/COMMUNITY_ACCESS.CLASS_SEARCH.GBLYou will need to select a specific academic term.

Academic Calendar

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

Campus Map

MS/CSEC courses are generally be held in the Golisano College of Computing & Information Sciences (GOL or building 70). RIT's various campus maps are available at facilities.rit.edu/campus/maps/.

MS/CSEC Program Worksheet (as of 2018-19)

Prerequisite Bridge Program [1]	Must be completed prior to start of program of study.
1 year of programming	
Discrete Mathematics	
Calculus – 1 year	
Statistics	
2 courses in natural sciences	
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)

Guidelines for Completion of a Program of Study:

This worksheet is sent to you when you are accepted into the MS in Computing Security (MS/CSEC). The RIT program code for this program is COMPSEC-MS. To earn the MS degree, you must complete the prerequisites and degree requirements shown on the front of this page. Contact the Graduate Director periodically to review your progress and receive an updated copy. If you lose your worksheet, the Student Services office can give you a current copy.

Applicable Notes:

Note #1: Prerequisite courses must be completed prior to beginning study in the MS program, typically within the first two terms after matriculation.

Note #2: Electives should be chosen in consultation with your graduate faculty. 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.

Note #3: The capstone may be a MS project or the capstone course (both 3 credits), or a MS thesis (6 credits).

Matriculation

When a student is accepted into the MS/CSEC program and registers for courses, the student is "matriculated" in this program of study and his/her academic status is "active."

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.

Inactive Status

If you have no registration activity in the term for which you were admitted, do not register for four (4) consecutive terms during your program of study, withdraw, or graduate, your academic status at RIT will become "inactive."

Discontinued Status

After four (4) consecutive terms without registration activity, 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. Contact the Graduate Director for assistance.

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 is does not apply to prerequisite courses.