# Enrollment Guide
# MS in Computing Security (Online)

## Table of Contents

1 What courses should I take? ........ 1

2 How do I search for courses? ........ 1

3 CSEC-MS Course Descriptions ........ 2

3.1 Fall Course Descriptions ........ 2

3.2 Spring Course Descriptions ........ 2

3.3 Summer Course Descriptions ........ 2

4 MS Computing Security Capstone ........ 3

4.1 CSEC 793 Capstone for Computing Security (3 credits) ........ 3

4.2 CSEC 791 MS Project (3 credits) ........ 3

**5 Who to Contact** ........ 3

## 1 What courses should I take?

You need to follow your program worksheet and/or your Academic Advising Report (AAR)

If you have been assigned one or more bridge (pre-requisite) courses, you must pass the course with a grade of "B" or better to have your bridge course requirements filled. Courses in your program of study will be considered successfully completed with a grade of "C" or higher, but please note that the minimum GPA required for a graduate student to remain in good academic standing and to graduate is a 3.0 or "B".

Please check with your academic advisor if you have any questions.

## 2 How do I search for courses?

**Searching for all courses**: see https://sis.rit.edu or https://tigercenter.rit.edu. All courses are coded with 4 letter subject codes. Courses offered by Computing Security, CSEC are listed as CSEC courses.

**General Enrollment Questions**: For more information regarding how to use SIS for Enrollment please view RIT's Enrollment Guide: https://www.rit.edu/infocenter/sites/rit.edu.infocenter/files/docs/2017-18%20Enrollment%20Guide%208-10-17.pdf

**Tiger Center:** A class search tool developed by RIT students in partnership with ITS is now available. Tiger Center has the same functionality as SIS but may be more intuitive when searching for classes. https://tigercenter.rit.edu

# 3 CSEC-MS Course Descriptions [Note that these apply to course options for online students only]

## 3.1 Fall Course Descriptions

**CSEC 604 Cryptography and Authentication (3 credits):**

In this course, students will learn in depth knowledge of cryptography and authentication. Students will explore various cryptography algorithms, authentication protocols, and their design and implementation. Students will work on a project to implement a cryptographic algorithm and/or an authentication protocol. The applications of cryptography and authentications in the areas of computer networks and systems and information assurance will also be investigated.

**CSEC 742 Computer system Security (3 credits):**

The importance of effective security policies and procedures coupled with experience and practice is emphasized and reinforced through research and practical assignments. Organization and management of security discipline and response to threats is studied. Case studies of effective and failed security planning and implementation will be examined and analyzed. The issues influencing proper and appropriate planning for security and response to attacks will be studied. To be successful in this course students should be knowledgeable in networking, systems, and security technologies.

## 3.2 Spring Course Descriptions

**CSEC 603 Enterprise Security (3 Credits)**

This course is designed to provide students with the advanced concepts needed to establish network security strategies to ensure adequate protection for the corporate environment and yet provide accessibility for the corporate community.

**CSEC 731 Web Server and Application Security Audits (3 credits)**

This course discusses the processes and procedures to perform a technical security audit of web servers and web-based applications. Students will not only explore Web Servers and Applications/Services threats, but also apply the latest auditing techniques to identify vulnerabilities existing in or stemming from web servers and applications. Students will write and present their findings and recommendations in audit reports on web servers and application vulnerabilities. To be successful in this course students should be knowledgeable in a scripting language and comfortable with the administration of both Linux and Windows platforms.

**CSEC 759 Graduate Seminar in Computing Security – Advanced Malware Forensics (3 credits)**

For adversaries today, malware is still the main attack vector to penetrate the defense and establish a foothold within enterprise networks. In this course, students will learn state-of-the-art techniques for malware analysis, detection, and anti-forensics. Topics include: the static, dynamic, and memory analysis of malware, along with malware evasion methods. Students will also study machine learning approaches for malware detection. They will investigate strength and weaknesses in traditional malware detection schemes, analyze and improve reported solutions in the literature.

### 3.3 Summer Course Descriptions

**CSEC 743 Computer Viruses and Malicious Software (3 credits):**

Computer malware is a computer program with malicious intent. In this course, students will study the history of computer malware, categorizations of malware such as computer viruses, worms, Trojan horses, spyware, etc. Other topics include, but are not limited to, basic structures and functions of malware, malware delivery mechanism, propagation models, anti-malware software, its methods and applications, reverse engineering techniques. Students will conduct research to understand the current state of the computer malware defense and offense.

Computer malware is a computer program with malicious intent. In this course, students will study the history of computer malware, categorizations of malware such as computer viruses, worms, Trojan horses, spyware, etc. Other topics include, but are not limited to, basic structures and functions of malware, malware delivery mechanism, propagation models, anti-malware software, its methods and applications, reverse engineering techniques. Students will conduct research to understand the current state of the computer malware defense and offense.

## 4 MS Computing Security Capstone

All graduate programs require a culminating experience, a capstone. Students can meet this requirement by successfully completing the capstone course or an independent capstone project.

### 4.1 CSEC 793 Capstone for Computing Security (3 credits)

The capstone course is offered to students each semester. Students must submit a two-page proposal for their project to the Graduate Director for approval. Students will apply their knowledge learned through the program to solve real world problems various areas of computing security. Large size projects will be defined for students to work on throughout the semester. At the end of semester students will present their results and demonstrate their knowledge and skills in problem solving and critical thinking in a setting open to the public.

### 4.2 CSEC 791 MS Project (3 credits)

The capstone project equates to three academic credits and is independent work completed under the supervision of two Computing Security faculty. Students complete a written project proposal with a completed literature review and specific deliverables which can be evaluated. It offers students the opportunity to investigate a selected topic within the computing security domain. The student may complete a project for real world application or in a laboratory environment. The project is evaluated during a capstone defense and at the submission of the final report, the student receives a grade for their capstone project.

## 5 Who to Contact

Please refer to http://www.rit.edu/gccis/computingsecurity/advising/graduate if you have any questions regarding what you read in this enrollment guide, or for any other reason, please contact your Academic Advisor ASAP.

Jill Persson jill.persson@rit.edu

You can call our front desk during normal business hours, Monday-Friday 8:30am to 4:30pm EST to schedule an appointment either over the phone or via SKYPE. The number is 585-475-2963.