CSEC 201: Programming for Info Sec.

Fall 2021

Instructor	Rob Olson
Office Location	Main CSEC Suite in GCI
E-mail	rboics@rit.edu
Office Hours	9:30am – 10:45 on T/Th
Course Time	Section 1: 11 AM – 12:15 PM on Tuesday & Thursday Section 4: 8 AM – 9:15 AM on Tuesday & Thursday
Course Place	GOL 2740

TAs	Michael Pothaczky mjp2960@rit.edu -- Be aware that any TA for any section can provide assistance
Office Hours	TBA
Place	Discord

1. **Catalog description:** This course builds upon basic programming skills to give students the programming knowledge necessary to study computing security. Students will be introduced to network programming, memory management, and operating system calls along with associated security concepts. Specific focus will be placed on understanding the compilation process and on the relation between high-level programming concepts and low-level programming concepts, culminating in identifying and exploiting memory corruption vulnerabilities.

2. Prerequisite(s): (CSEC 101 or CSEC 140) and (CSCI 142 or CSEC/SWEN 124)

3. Required Course Textbook: None

4. Recommended Supplemental Textbooks

- Hacking: The Art of Exploitation, Jon Erickson, No Starch Press, 2008
- Black Hat Python: Python Programming for Hackers and Pentesters, Justin Seitz, No Starch Press, 2014
- Shellcoder's Handbook: Discovering and Exploiting Security Holes, Anley; Heasman; Leindner; Richarte, Wiley, 2007
- The Linux Programming Interface, Michael Kerrisk, No Starch Press, 2010

5. Course Objective: The primary goal of this course is to provide students with an introduction to core application security concepts while, at the same time, teaching students the programming skills they will need in

the information security profession. The secondary goal of this course is to provide students with a broad exposure to relevant high and low-level programming languages used in information security.

6. Learning Outcomes

After completing this course, the student will be able to:

Course Learning Outcome	Assessment Method
Students will be able to program using sockets in multiple languages.	Multiple programming assignments
Students will understand of how memory can and should be managed programmatically.	Programming assignment
Students will understand the compilation process and how high-level code is translated into low-level code.	Programming assignment
Students will be able to write basic programs in a low-level programming language such as x86 assembly.	Programming assignment
Students will have an understanding of how memory corruption vulnerabilities can be exploited and be able to write basic memory corruption exploits.	Programming assignment

7. Tentative Course Outline

Week 1:	Threading and multiprocessing in Python	Lab 1: Threading and Multiprocessing
Week 2:	OS and Sockets in Python	Lab 2: Python Socket Programming
Week 3:	Data types, Pointers, Arrays in C	Lab 3: A block cipher in C
Week 4:	Data structures	Lab 4: Data structures in C
Week 5:	Vulnerabilities, Function Pointers	Lab 5: Blockchain
Week 6:	Linux Sys. Programming	Lab 6: Linux Sys. Programming
Week 7:	Linus/Windows Sys. Programming	Lab 7: Windows Programming
Week 8:	Midterm	
Week 9:	More Windows Sys. Programming	Lab 8: Windows Programming or Debugging (TBD)
Week 10:	x86 Assembly	Lab 9: Assembly lab #1
Week 11:	x86 Assembly	Lab 10: Assembly lab #2
Week 12:	x86 Assembly	Lab 11: Assembly lab #3
Week 13:	Fuzzing	Lab 12: Writing a fuzzer
Week 14:	Exploiting stack overflows	Lab 13: Completing the exploit
Week 15:	Modern Memory Protection Techniques (DEP/ASLR/Canaries/CFG/etc)	

8. Course Structure:

This course will combine lecture and in-class learning activities, and out of class assignments to be completed individually.

9. Grading:

The relative weight of each component of your grade is shown on the table below.

Component	**Percentage**
In-class activities (including attendance)	27%
Labs	39%
Exams (Midterm/Final)	34%

The table below lists student's grade for a given percentage achieved. Numeric grades that fall between categories will be rounded up or down at the discretion of the instructor.

94%-100%	90%-93%	88%-89%	82%-87%	80%-81%	78%-79%	72%-77%	70%-71%	60%-69%	0%-59%
A	A-	B+	B	B-	C+	C	C-	D	Fail

10. In-class Activities

The deadline for in-class activity submissions is 11:59 PM on the same day they were assigned. You are strongly encouraged to push your solutions to GitHub before the end of the class period. Your TAs will grade your in-class activities by verifying that you submitted your solutions to GitHub before the deadline. **No extension** will be allowed to any individual students under any circumstances.

11. Lab Submissions

A lab is posted on Tuesday and is due at 7 PM on Wednesday on the following week. For each lab, you must meet one of the TAs or instructors to receive sign-offs AND submit final source code for the assignment to GitHub before7 PM on Wednesday.

It is expected that lab sign-offs will be acquired during (virtual or in-person) office hours. Students should understand that coming to office hours at the last minute with little work done on the lab will likely not result in sign-offs. Students are encouraged to come to take extensive notes on lecture material, to start assignments as soon as they are given, and to come to office hours early.

12. Late Policy for lab and exams

All exams must be taken on the day that they are given. All lab assignments are due on the date listed in the hand-out provided by the instructor. No exceptions will be made, except for excused absences. Excused absences will be granted for the reasons such as the following and require written documentation:

1. Illness of the student or serious illness of a member of the student's immediate family.
2. A death in the student's immediate family
3. Trips sponsored by official RIT student groups, academic units, or athletic teams.
4. Major religious holidays

A student requiring special considerations for reasons 3 or 4 should talk to the instructor at least a week in advance.

13. Academic Honesty

The following is taken from the RIT policy on academic honesty[1]:

> "A breach of student academic integrity falls into three basic areas: cheating, duplicate submission and plagiarism
>
> A. Cheating: Cheating is any form of fraudulent or deceptive academic act, including falsification of data, possessing, providing, or using unapproved materials, sources, or tools for a project, exam, or body of work submitted for faculty evaluation.
>
> B. Duplicate Submission: Duplicate submission is the submitting of the same or similar work for credit in more than one course without prior approval of the instructors for those same courses.
>
> C. Plagiarism: Plagiarism is the representation of others' ideas as one's own without giving proper attribution to the original author or authors. Plagiarism occurs when a student copies direct phrases from a text (e.g. books, journals, and internet) and does not provide quotation marks or paraphrases or summarizes those ideas without giving credit to the author or authors. In all cases, if such information is not properly and accurately documented with appropriate credit given, then the student has committed plagiarism."

Potential punishments for academic dishonesty may include:

- Receiving a failing grade on an assignment
- Failing the course
- Dismissal from the university

14. COVID-19 Syllabus Addendum

- We are all aware of the unique circumstances of this fall semester resulting from the worldwide COVID-19 SARS-2 pandemic. RIT has consulted federal, state, and local guidelines and policies to implement a safe, yet educational environment for students, faculty and staff. These guidelines, located at https://www.rit.edu/ready/ are routinely updated as conditions change.

[1] The policy on academic honesty can be found at https://www.rit.edu/academicaffairs/policiesmanual/d080

- What do these mean for this class? When we meet in person everyone will wear a mask that covers their mouth and nose at all times and have freshly washed or sanitized hands. In class, students will sit in assigned seats in the locations designated by faculty. We will not congregate in hallways, bathrooms or classrooms prior to or after class. Any presence of fever or other COVID-19 symptoms will be reported on the RIT Daily Health Screen Monitoring https://www.rit.edu/news/rit-launches-daily-health-screen-monitoring-covid-19-symptoms; please notify your instructor so that the best way to accommodate your learning can be planned.

- Students are expected to fully honor the RIT Ready Pledge and put on a mask. In the event the student fails to put on a mask, then the student will be asked to leave class.

- Should a student fail to adhere to instructor's request to fully honor the RIT Ready Pledge and classroom procedures OR promptly leave the classroom as requested, in the interest of health and safety, Public Safety can be called to assist in addressing the matter.

15. COURSE SUCCESS

Success in this course depends heavily on your personal health and wellbeing. Recognize that stress is an expected part of the college experience, and it often can be compounded by unexpected setbacks or life changes outside the classroom. Moreover, those with marginalized identities may be faced with additional social stressors. Your other instructors and I strongly encourage you to reframe challenges as an unavoidable pathway to success. Reflect on your role in taking care of yourself throughout the term, before the demands of exams and projects reach their peak. Please feel free to reach out to me about any difficulty you may be having that may impact your performance in this course as soon as it occurs and before it becomes unmanageable. In addition to your academic advisor, I strongly encourage you to contact the many other support services on campus that stand ready to assist you.