



## ENPM691 Hacking of C Programs and Unix Binaries (0101, DE01)

**Term:** Fall 2024

**Professor:** Dr. W. Lewis Collier

Pronouns: he/him

Office Phone: N/A

**Email:** [lcollier@umd.edu](mailto:lcollier@umd.edu)

**Office Hours:** Friday (before/after class) & by appointment

Credits: 3

**Course Dates:** From 26 August 2024 – 17 December 2024

**Course Times:** Friday 2:00 - 4:40 pm and Online

Classroom: JMP **TBD**

Canvas/ELMS: <https://umd.instructure.com/courses/1374651>

### Course Description

This course teaches the fundamentals of secure programming in C. An in-depth discussion on various security vulnerabilities (e.g., buffer overflows) in C applications will be taught with a hands-on demo of concepts during the class. Students will learn how a C program runs “under-the-hood”. The course will teach nitty-gritty of C programs by analyzing at the assembly level. The course discusses best practices (e.g., coding standards) and design principles for secure programming so that security can be built-in during design time.

### Prerequisites

- Equivalent of ENEE 150.

Students taking this course must have prior knowledge of C/C++. In particular, this course assumes that students are familiar with basic programming constructs such as control flow, loops, arrays, structures, pointers, and File I/O. If you have not programmed in C but used other similar programming languages, you may talk to the instructor, but all assignments utilize C.

Familiarity with the UNIX environment will be very helpful. If you are not familiar or experienced with UNIX, complete at least the first 15 levels of the Over the Wire Wargames “Bandit” Challenge to build some core fundamentals. Familiarization with the Python programming language is also a bonus.

The course requires a fair amount of effort to keep up with the pace of the class. It is a highly technical class. Students should be prepared to devote time to gain the most!

## Learning Outcomes

After successfully completing this course, you will be able to:

- Understand the fundamentals of secure programming.
- Perform security attacks (e.g., buffer overflows, format string vulnerabilities).
- Debug C programs and understand “under the hood” behavior.
- Learn machine/assembly representation of C programs.
- Analyze C programs for security vulnerabilities.
- Understand core differences between 32-bit and 64-bit assembly.
- Explain the problem being investigated, steps to analyze it, and the solution.

## Course Materials

This course will leverage the following resources. Many textbooks will be referenced because this course requires the student to learn the fundamentals of computer systems from a programmer’s perspective, assembly level programming and debugging. These mandatory skills for secure programming are often not fully described in a single book. Thus, we will cover selected chapters from each of the following books. In addition, we may refer to several online materials (e.g., blogs, presentations, user manuals of Intel IA32/IA64, GNU tools, etc.)

Students need not buy all the following books. The slides and demos of our lectures should be sufficient in general.

- Brian Kernighan and Dennis Ritchie. The C Programming Language, 2nd Edition.
- Randy Bryant’s and David R. O’Hallaron. Computer Systems: A Programmer’s Perspective, 2nd Edition.
- Robert Seacord. Secure Coding in C and C++, 1st Edition.
- K. N. King. C Programming. A Modern Approach. W. W. Norton & Company.

Additionally, there are some very helpful open-source resources that can help supplement your understanding of course material, including various [YouTube videos](#).

## Computing Requirements

\*\*\* YOU MUST HAVE AN x86 BASED PROCESSOR. \*\*\*

\*\*\* M1/M2 MACs (ARM based MACs) will NOT work for this course. \*\*\*

It is assumed that the students will have access to a laptop which can run virtual machines (VMs). During the class, the instructor will use Kali Linux VM on a VMWare Workstation Hypervisor that can be obtained through Terpware/Kivoto for free. A pre-configured VM will be provided to students. Occasionally a 64-bit version will also be used to demonstrate some concepts to show differences to 32-bit representations. We will also provide virtual machines for you during the first weeks of the semester. Debugging will be based on GNU’s GDB, with exploit development plugins such as pwndbg. All C programs will be compiled using GNU’s C compiler. Reverse engineering and static analysis will be done through Ghidra. The instructor will use the Intel syntax for teaching assembly language representations of C programs. Occasionally the AT&T syntax will be used to highlight differences to the Intel syntax.

## Course Structure

This course includes both on-campus and online sections. To attend synchronously online, log into ELMS-Canvas at the time of the Section 0101 class and select “Video Conference” from the left side menu. This will open a Zoom link to the live classroom.

For asynchronous online students, all lectures will be recorded and made available on ELMS-Canvas under “Panopto Recordings/Video Lectures” within 24 hours of the class time. Be sure to review the recorded lecture in a timely manner.

**Please note** that F1 students enrolled in the on-campus section are required to attend in person. If you have a conflict on a particular day, please reach out to me in advance to discuss.

On-campus students should come to class prepared to engage with the lecture and materials. Online students, be sure to log onto Canvas regularly and participate in discussions and activities. Regardless of the section you are enrolled in, participation is expected.

Each lecture period will be divided into three parts: Lecture, overview of programming exercise (homework), and in-class work time/Q&A.

The course is structured so that group efforts are used in the beginning of the assignments, with all learning assessment products to be completed by individual efforts. The intent is that the group members work together to get up to speed on the development tools and methodologies. Group collaboration is encouraged for individual projects, but ALL work products are to be created as individual efforts. This ensures that all students wind up with a set of well-understood artifact templates for future use in all their design efforts.

## Homework Assignments

This course will have 12 programming assignments, mostly each week (50%), a mid-term (20%), and a final exam (30%). The programming assignments will allow students to put into practice the topic(s) from that week’s lecture, and prior material. Each assignment’s submission will include a “lab report” where the student outlines their code and lessons learned. The mid-term will cover the material from the first half of the semester and the final will cover all material with an emphasis on the material covered since the midterm.

Each homework assignment will be exploratory in nature. Each lecture covers topics about how computer programming structures work. The homework assignments provide an opportunity for the students to understand attack vectors for software programs so they can be avoided in real-world programming. These explorations also give rise to a deeper understanding of how computer programs work in detail. The homework assignments include writing a lab report that defines the attack vector hypothesis, the analysis of the vector, and mitigation results.

Students are encouraged to work with each other to get started on each weekly assignment during the in-class work time, but all work must be completed individually. The in-class work time allows for students to begin working on assignments, if they wish, to allow for direct feedback from the instructor and peer learning from fellow classmates.

## Communication Guidelines

### Communicating with the Instructor

My goal is to be readily available to you throughout the semester. I can be reached by email at lcollier@umd.edu. Please DO NOT email me with questions that are easily found in the syllabus or on ELMS-Canvas (e.g., When is this assignment due? How much is it worth? etc.), but please DO reach out about personal, academic, and intellectual concerns/questions.

While I will do my best to respond to emails within 24 hours, you will more likely receive email responses from me on between 5pm and 9pm Monday through Thursday evenings.

When constructing an email to me please put "ENPM691: Your Topic" in the subject line. This will draw my attention to your email and enable me to respond to you more quickly.

Additionally, please review [These tips for 'How to email a Professor'](#). By following these guidelines, you will be ensured to receive a timely and courteous response.

Finally, if you need to discuss issues not appropriate for the classroom and/or an email, we can arrange to talk by phone, over Zoom, or in person. Send me an email asking for a meeting and we can set something up.

### Announcements

I will send IMPORTANT messages, announcements, and updates through ELMS-Canvas. To ensure you receive this information in a timely fashion, make sure your email and announcement notifications (including changes in assignments and/or due dates) are enabled in ELMS-Canvas ([How to change notification settings in CANVAS](#)).

Log into our ELMS-Canvas course site at least once every 24-hour period to check your inbox and the Announcements page.

### Names/Pronouns and Self-Identifications

The University of Maryland recognizes the importance of a diverse student body, and we are committed to fostering inclusive and equitable classroom environments. I invite you, if you wish, to tell us how you want to be referred to in this class, both in terms of your name and your pronouns (he/him, she/her, they/them, etc.). Keep in mind that the pronouns someone uses are not necessarily indicative of their gender identity. Visit [trans.umd.edu](http://trans.umd.edu) to learn more.

Additionally, it is your choice whether to disclose how you identify in terms of your gender, race, class, sexuality, religion, and dis/ability, among all aspects of your identity (e.g., should it come up in classroom conversation about our experiences and perspectives) and should be self-identified, not presumed or imposed. I will do my best to address and refer to all students accordingly, and I ask you to do the same for all of your fellow Terps.

### Communicating with your Peers

With a diversity of perspectives and experience, we may find ourselves in disagreement and/or debate with one another. As such, it is important that we agree to conduct ourselves in a professional manner and that we work together to foster and preserve a virtual classroom environment in which we can respectfully discuss and deliberate controversial questions. I

encourage you to confidently exercise your right to free speech—bearing in mind, of course, that you will be expected to craft and defend arguments that support your position. Keep in mind, that free speech has its limit and this course is NOT the space for hate speech, harassment, and derogatory language. I will make every reasonable attempt to create an atmosphere in which each student feels comfortable voicing their argument without fear of being personally attacked, mocked, demeaned, or devalued.

Any behavior (including harassment, sexual harassment, and racially and/or culturally derogatory language) that threatens this atmosphere will not be tolerated. Please alert me immediately if you feel threatened, dismissed, or silenced at any point during our semester together and/or if your engagement in discussion has been in some way hindered by the learning environment.

### **Netiquette Policy**

Netiquette is the social code of online classes. Students share a responsibility for the course’s learning environment. Creating a cohesive online learning community requires learners to support and assist each other. To craft an open and interactive online learning environment, communication has to be conducted in a professional and courteous manner at all times, guided by common sense, collegiality and basic rules of etiquette.

## **Grading**

### **Grade Breakdown**

Assignment	Percentage %
12 Homework Assignments	50%
Midterm Examination	20%
Final Exam	30%
Total	100%

### **Grading Assignments**

All assignments will be graded according to a predetermined set of criteria (i.e., rubric) which will be communicated to students before the assignment is submitted.

To progress satisfactorily in this class, students need to receive timely feedback. To that end, it is my intention to grade all assignments within **a week from** their due date. If an assignment is taking longer than expected to grade, students will be informed of when they can expect to see their grade.

### **Grade Computation**

All assessment scores will be posted on ELMS/Canvas page. If you would like to review any of your grades (including the exams), or have questions about how something was scored, please email me to schedule a time for us to meet and discuss.

It is expected that you will submit work by the deadline listed in the syllabus and/or on ELMS-Canvas. Late work will be penalized according to the late work policy described in the **Course Policies and Procedures** section below.

**Grade Disputes:** I am happy to discuss any of your grades with you, and if I have made a mistake, I will immediately correct it. Any formal grade disputes must be submitted in writing and within one week of receiving the grade.

Final letter grades are assigned based on the weighted percentage of total assessment points earned. Final grades will be tabulated from the weighted averages, rounding upwards from fractional values. Thus, an average of 97.51 would equate to a letter grade of A+ and an average of 97.50 would equate to a letter grade of A. To be fair to everyone I have to establish clear standards and apply them consistently, so please understand that being close to a cutoff is not the same this as making the cut. It would be unethical to make exceptions for some and not others.

Final Grade Cutoffs									
+	>97.50%	+	>87.50%	+	>77.50%	+	>67.50%	+	
A	92.50% to 97.50%	B	82.50% to 87.5	C	72.50% to 77.50%	D	62.50% to 67.50%	F	<60.0%
-	>=90.00%	-	>= 80.00%	-	>=70.00%	-	>=60.00%	-	

## Course Schedule

Week 01	30 Aug 2024
Before Class	
a) Review Slides for Week 1	
Topics :: Intro to Course	
After Class:	
a) <u>Complete</u> Assignment 1	
b) Review Slides for Week 2	

Week 02	06 Sep 2024
Before Class	
a) Review Slides for Week 2	
Topics :: Intro to Course	
After Class:	
a) <u>Complete</u> Assignment 2	
b) Slides for Week 3	

Week 03	13 Sep 2024
Before Class	
a) Review Slides for Week 3	
Topics :: Intro to Course	
After Class:	
a) <u>Complete</u> Assignment 3	
b) Review Slides for Week 4	

Week 04	20 Sep 2024
Before Class	
a) Review Slides for Week 4	
Topics :: Intro to Course	
After Class:	
a) <u>Complete</u> Assignment 4	
b) Review Slides for Week 5	

Week 05	27 Sep 2024
Before Class	
a) Review Slides for Week 5	
Topics :: Intro to Course	
After Class:	
a) <u>Complete</u> Assignment 5	
b) Review Slides for Week 6	

Week 6	04 Oct 2024
Before Class	
b) Review Slides for Week 6	
Topics :: Intro to Course	
After Class:	
c) <u>Complete</u> Assignment 6	
d) Review Slides for Week 7	

Week 7	11 Oct 2024
Before Class	
a) Review Slides for Week 7	
Topics :: Intro to Course & Midterm Review	
After Class:	
a) <u>Complete</u> Midterm Exam	
b) Review Slides for Week 8	

Week 8	18 Oct 2024
Before Class	
a) Review Slides for Week 8	
Topics :: Intro to Course	
After Class:	
a) <u>Complete</u> Assignment 7	
b) Review Slides for Week 9	

Week 9	25 Oct 2024
Before Class	
a) Review Slides for Week 9	
Topics :: Intro to Course	
After Class:	
a) <u>Complete</u> Assignment 8	
b) Review Slides for Week 10	

Week 10	01 Nov 2024
Before Class	
a) Review Slides for Week 10	
Topics :: Intro to Course	
After Class:	
a) <u>Complete</u> Assignment 9	
b) Review Slides for Week 11	



Week 11	08 Nov 2024
Before Class	
a) Review Slides for Week 11	
Topics :: Intro to Course	
After Class:	
a) <i>Complete</i> Assignment 10	
b) Review Slides for Week 12	

Week 12	15 Nov 2024
Before Class	
a) Review Slides for Week 12	
Topics :: Intro to Course	
After Class:	
a) <i>Complete</i> Assignment 11	
b) Review Slides for Week 13	

Week 13	22 Nov 2024
Before Class	
a) Review Slides for Week 13	
Topics :: Intro to Course	
After Class:	
a) <i>Complete</i> Assignment 12	
b) Review Slides for Week 15	

Week 14	29 Nov 2024 (NO CLASS Thanksgiving Break)
---------	---

Week 15	06 Dec 2024 (Last day of classes)
Before Class	
a) Review Slides for Week 15	
Topics :: Intro to Course & Final Exam Review	
After Class:	
a) Study for Final Exam	

Week 16	11 - 17 Dec 2024 Final Exams (Due date TBD)
Before Class:	
a) Complete Final Exam	
Final Exam	
After Exam:	
a) Relax	
b) Finish the semester strong in your other courses!	

Note: This is a tentative schedule, and subject to change as necessary due to weather delays, etc. Monitor ELMS-Canvas for current deadlines. In the unlikely event of a prolonged university closing, or an extended absence from the university, adjustments to the course schedule, deadlines, and assignments will be made based on the duration of the closing and the specific dates missed.

## Course Policies and Procedures

The University of Maryland's conduct policy indicates that course syllabi should refer to a webpage of course-related policies and procedures. For a complete list of graduate course related policies, visit the [Graduate School website](#). Below are course-specific policies and procedures which explain how these Graduate School policies will be implemented in this class.

## Classroom Technology

I expect you to make the responsible and respectful decision to refrain from using your cellphone during class time. If you have critical communication to attend to, please excuse yourself and return when you are ready. For more information about the science behind the policy watch: <http://youtu.be/WwPaw3Fx5Hk>

Likewise, as I do not expect students to be buried in their computers, this will not be a PowerPoint presentation-centric course. I will use slides to highlight topics, and data sets, but I will not be reading them to you. I expect students to have read the material before the class so that in-depth discussions can be had during class. As stated above, the overarching goal of this class is to provide an understanding of embedded systems design and optimization. Hands on practice will lead to a better understanding when real systems are developed, but discussion beforehand will afford the base understanding that enables the deeper comprehension when development is performed, and design artifacts are created.

## **Satisfactory Performance**

The Graduate School expects students to take full responsibility for their academic work and academic progress. The student, to progress satisfactorily, must meet all the academic requirements of this course. Additionally, each student is expected to complete all readings and any preparatory work before each class session, come to class prepared to make substantive contributions to the learning experience, and to proactively communicate with the instructor when challenges or issues arise.

## **Questions about Assignments**

Please ask all questions you may have about an assignment by 9:00 PM the Friday before the assignment due date (which is usually Monday at start of class). Any questions asked after that time may not be answered in time for you to make changes to your work.

## **Late Work Policy**

Assignments should be completed by the due date and time listed with the assignment, on the syllabus, and/or in the course calendar. If you are unable to complete an assignment by the stated due date, it is your responsibility to contact your instructor to discuss an extension, at least 24 hours BEFORE the assignment is due. Extensions are not guaranteed but may be granted at the instructor's discretion.

Assignments submitted late without an approved extension may receive a 10% deduction in total grade per each calendar day late up to a maximum of three days late (i.e., there is a maximum of a 30% grade reduction for assignments submitted late). Work submitted more than three days late without an approved extension may not receive feedback and may automatically earn a grade of zero.

## **Religious Observance**

It is the student's responsibility to inform the instructor of any intended absences for religious observances in advance. Notice should be provided as soon as possible but no later than the end of the schedule adjustment period.

## **Academic Integrity**

For this course, some of your assignments may be collected via Turnitin on ELMS/Canvas. I have chosen to use this tool because it can help you improve your scholarly writing and help me verify the integrity of student work. For information about Turnitin, how it works, and the feedback reports you may have access to, visit [Turnitin Originality Checker for Students](#)







The University's Code of Academic Integrity is designed to ensure that the principles of academic honesty and integrity are upheld. In accordance with this code, the University of Maryland does not tolerate academic dishonesty. Please ensure that you fully understand this code and its implications because all acts of academic dishonesty will be dealt with in accordance with the provisions of this code. All students are expected to adhere to this Code. It is your responsibility to read it and know what it says, so you can start your professional life on the right path. **As future professionals, your commitment to high ethical standards and honesty begins with your time at the University of Maryland.**

It is important to note that course assistance websites, such as CourseHero, or AI generated content are not permitted sources, unless the instructor explicitly gives permission. Material taken or copied from these sites can be deemed unauthorized material and a violation of academic integrity. These sites offer information that might be inaccurate or biased and most importantly, relying on restricted sources will hamper your learning process, particularly the critical thinking steps necessary for college-level assignments.

Additionally, students may naturally choose to use online forums for course-wide discussions (e.g., Group lists or chats) to discuss concepts in the course. However, **collaboration on graded assignments is strictly prohibited unless otherwise stated**. Examples of prohibited collaboration include: asking classmates for answers on quizzes or exams, asking for access codes to clicker polls, etc. Please visit the [Office of Graduate Studies' full list of campus-wide policies](#) and reach out if you have questions.

Finally, on each exam or assignment you must write out and sign the following pledge: "I pledge on my honor that I have not given or received any unauthorized assistance on this exam/assignment." If you ever feel pressured to comply with someone else's academic integrity violation, please reach out to me straight away. Also, **if you are ever unclear** about acceptable levels of collaboration, **please ask!**

To help you avoid unintentional violations, **the following table** lists levels of collaboration that are acceptable for each graded exercise.

	 <b>OPEN NOTES</b>	 <b>USE BOOK</b>	 <b>LEARN ONLINE</b>	 <b>GATHER CONTENT With AI</b>	 <b>ASK FRIENDS</b>	 <b>WORK IN GROUPS</b>
Assignments	✓	✓	✓	X	✓	X
Exams	✓	✓	X	X	X	X

### Course Evaluation

Please submit a course evaluation through Student Feedback on Course Experiences in order to help faculty and administrators improve teaching and learning at Maryland. All information submitted to Course Experiences is confidential. Campus will notify you when Student Feedback on Course Experiences is open for you to complete your evaluations at the end of the semester. Please go directly to the [Student Feedback on Course Experiences](#) to complete your evaluations. By completing all of your evaluations each semester, you will have the privilege of accessing through Testudo the evaluation reports for the thousands of courses for which 70% or more students submitted their evaluations.

### Copyright Notice

Course materials are copyrighted and may not be reproduced for anything other than personal use without written permission.

## Tips for Succeeding in this Course

1. **Participate.** I invite you to engage deeply, ask questions, and talk about the course content with your classmates. You can learn a great deal from discussing ideas and perspectives with your peers and professor. Participation can also help you articulate your thoughts and develop critical thinking skills.
2. **Manage your time.** Students are often very busy, and I understand that you have obligations outside of this class. However, students do best when they plan adequate time that is devoted to course work. Block your schedule and set aside plenty of time to complete assignments including extra time to handle any technology related problems.
3. **Login regularly.** I recommend that you log in to ELMS-Canvas several times a week to view announcements, discussion posts and replies to your posts. You may need to log in multiple times a day when group submissions are due.
4. **Do not fall behind.** This class moves at a quick pace and each week builds on the previous content. If you feel you are starting to fall behind, check in with the instructor as soon as possible so we can troubleshoot together. It will be hard to keep up with the course content if you fall behind in the pre-work or post-work.
5. **Use ELMS-Canvas notification settings.** Pro tip! Canvas ELMS-Canvas can ensure you receive timely notifications in your email or via text. Be sure to enable announcements to be sent instantly or daily.
6. **Ask for help if needed.** If you need help with ELMS-Canvas or other technology, IT Support. If you are struggling with a course concept, reach out to me and your classmates for support.

## Student Resources and Services

Taking personal responsibility for your learning means acknowledging when your performance does not match your goals and doing something about it. I hope you will come talk to me so that I can help you find the right approach to success in this course, and I encourage you to visit the [Counseling Center's Academic Resources](#) to learn more about the wide range of resources available to you. Below are some additional resources and services commonly used by graduate students. For a more comprehensive list, please visit the Graduate School's [Campus Resources Page](#).

### Accessibility and Disability Services

The University of Maryland is committed to creating and maintaining a welcoming and inclusive educational, working, and living environment for people of all abilities. The University of Maryland is also committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of the University, or be subjected to discrimination. The [Accessibility & Disability Service \(ADS\)](#) provides reasonable accommodations to qualified individuals to provide equal access to services, programs and activities. ADS cannot assist retroactively, so it is generally best to request accommodations several weeks before the semester begins or as soon as a disability becomes known. Any student who needs accommodations should contact me as soon as possible so that I have sufficient time to make arrangements.

For assistance in obtaining an accommodation, contact Accessibility and Disability Service at 301-314-7682, or email them at [adsfrontdesk@umd.edu](mailto:adsfrontdesk@umd.edu). Information about [sharing your accommodations with instructors, note taking assistance](#) and more is available from the [Counseling Center](#).

## **Writing Center**

Everyone can use some help sharpening their communication skills (and improving their grade) by visiting [The Graduate School's Writing Center](#) and schedule an appointment with them.

Additionally, international graduate students may want to take advantage of the Graduate School's free [English Editing for International Graduate Students \(EEIGS\) program](#).

## **Health Services**

The University offers a variety of physical and mental health services to students. If you are feeling ill or need non-emergency medical attention, please visit the [University Health Center](#).

If you feel it would be helpful to have someone to talk to, visit [UMD's Counseling Center](#) or [one of the many other mental health resources on campus](#).

## **Notice of Mandatory Reporting**

Notice of mandatory reporting of sexual assault, sexual harassment, interpersonal violence, and stalking: As a faculty member, I am designated as a "Responsible University Employee," and I must report all disclosures of sexual assault, sexual harassment, interpersonal violence, and stalking to UMD's Title IX Coordinator per University Policy on Sexual Harassment and Other Sexual Misconduct.

If you wish to speak with someone confidentially, please contact one of UMD's confidential resources, such as [CARE to Stop Violence](#) (located on the Ground Floor of the Health Center) at 301-741-3442 or the [Counseling Center](#) (located at the Shoemaker Building) at 301-314-7651.

You may also seek assistance or supportive measures from UMD's Title IX Coordinator, Angela Nastase, by calling 301-405-1142, or emailing [titleIXcoordinator@umd.edu](mailto:titleIXcoordinator@umd.edu).

To view further information on the above, please visit the [Office of Civil Rights and Sexual Misconduct's](#) website at [ocrsm.umd.edu](http://ocrsm.umd.edu).

## **Basic Needs Security**

If you have difficulty affording groceries or accessing sufficient food to eat every day, or lack a safe and stable place to live, please visit [UMD's Division of Student Affairs website](#) for information about resources the campus offers you and let me know if I can help in any way.

## **Veteran Resources**

UMD provides some additional supports to our student veterans. You can access those resources at the office of [Veteran Student life](#) and the [Counseling Center](#). Veterans and active duty military personnel with special circumstances (e.g., upcoming deployments, drill requirements, disabilities) are welcome and encouraged to communicate these, in advance if possible, to the instructor.