MARYLAND APPLIED GRADUATE ENGINEERING

Hacking of C Programs and Unix Binaries (ENPM 691)
Sections 0101 and CY01

Professor: Dr. Dharmalingam Ganesan
Email: dganesan@umd.edu
Office Hours: TBD

Grader: Dhiral Manilaben Vyas
Email: dvyas1@umd.edu
Office Hours: TBD

Term: Spring 2024
Credits: 3
Course Dates: From January 26th – May 17th

Course Times
Sections 0101 and CY01: Fridays 2:00 - 4:40 PM

Classroom
Section 0101: JMP 2121

Canvas ELMS Link: https://umd.instructure.com/courses/1360068

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
There are no official prerequisites, however, students taking this course should have prior knowledge of C. In particular, this course assumes that students are familiar with basic C 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. Some familiarity with the UNIX environment will also be helpful. 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:

- Explain the fundamentals of secure programming.
- Perform security attacks (e.g., buffer overflows, format string vulnerabilities).
- Debug C programs and understand "under the hood" behavior.
- Correlate machine/assembly instructions with the corresponding C programs.

- Analyze C programs for security vulnerabilities.
- Differentiate between 32-bit and 64-bit assembly.

Recommended Reading 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.

- 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.
- Brian Kernighan and Dennis Ritchie. The C Programming Language, 2nd

Computing Requirements

It is assumed that the students will have access to a laptop which can run virtual machines. During the class, the instructor will use Ubuntu Linux VMWare on a 32-bit machine. However, 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. Students may use the CD that comes with the book of Jon Erickson (see above) for installing/running a Linux version on their machines. Debugging will be based on GNU's GDB. All C programs will be compiled using GNU's C compiler. The instructor will use the AT&T syntax for teaching assembly language representations of C programs. Occasionally the Intel syntax will be used to highlight differences to the AT&T syntax.

Course Structure

This course includes both on-campus and online sections.

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. If online students wish to attend synchronously online, you can do so by logging into ELMS-Canvas at the time of the Section 0101 class [Fridays 2:00 - 4:40 PM] and selecting "Video Conference" from the left side menu. This will open a Zoom link to the live classroom.

On-campus students are expected to attend in-person class sessions and be prepared to engage with the lecture and materials. If you have a conflict on a particular day, please reach out to me in advance to discuss. Online students, be sure to log into Canvas regularly and participate in discussions and activities. Regardless of the section you are enrolled in, participation is expected.

Please note that F1 students enrolled in the on-campus section are required to attend in person.

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 dganesan@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. I will do my best to respond to emails within 48 hours. When constructing an email to me please put "ENPM 691 (Section XXXX): 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 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 %
Homework	**50%**
Quizzes	**25%**
Final Exam	**25%**
Total	**100%**

Course Assignments

Homework Assignments

The course requires students to complete 3 homework assignments. Homeworks will generally be similar to the format of weekly quizzes, with the students having until the deadline for submission without any time limit.

Quizzes

There will be 1 quiz every week unless explicitly mentioned otherwise. These quizzes will be for 45-60 minutes and are designed to test the knowledge of students based on the subject material taught the previous week and the weeks before. Students can expect theoretical questions related to how C works as well as questions related to binary analysis and exploitation as part of these quizzes.

Final Exam

The final exam pattern will be similar to the weekly quizzes and will contain theoretical questions as well as questions related to binary analysis and exploitation. The final exam will be conducted simultaneously for all sections of the course. In-person students are expected to take the final in class. For more information regarding the time and location of the final exam, visit Fall 2023 Final Examination Tables.

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 **1 week** of 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 percentage of total assessment points earned. 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 as making the cut (89.99 ≠ 90.00). It would be unethical to make exceptions for some and not others. In this course, I use **Absolute Grading**

A+: 95 <= score <= 100
A: 90 <= score < 95
A-: 85 <= score < 90

B+: 80 <= score < 85
B: 75 <= score < 80
B-: 70 <= score < 75

C+: 65 <= score < 70
C: 60 <= score < 65
C-: 50 <= score < 60

D: 0 <= score < 50

Course Schedule

Week #	Topics	Assignments and Deliverables
1 **26th Jan –** **1st Feb**	**Motivation for Secure Programming** Software Security – Why? Example Vulnerabilities A Tour of Computer Systems	**Quiz 1**

2 **2nd Feb -** **8th Feb**	**Foundations- 1** Bits and Bytes Hexadecimal Notation Addressing and Byte Ordering	**Quiz 2**
3 **9th Feb -** **15th Feb**	**Foundations - II** Integer Security Integer Arithmetic Integer Overflow and Security Vulnerabilities	**Quiz 3**
4 **16th Feb –** **22nd Feb**	**Machine-Level Representation of C programs - I** Tour of Assembly Language	**Quiz 4**
5 **23rd Feb –** **29th Feb**	**Machine-Level Representation of C programs - II** Conditional Statements, Switch-Case Statements, Loops	**Quiz 5**
6 **1st Mar -** **7th Mar**	**Introduction to 64-bit Assembly**	**Quiz 6**
7 **8th Mar -** **14th Mar**	**Stack-based Buffer Overflow** Function calls and Stack Layout Representation of buffers at the assembly level Smashing the stack Protecting the stack	**Quiz 7** **Homework 1 released**
8 **15th Mar –** **21st Mar**	**Data Pointer and Function Pointer Vulnerabilities** Smashing the stack by exploiting pointers Dynamic memory allocation and security	**Quiz 8**
9 **22nd Mar –** **28th Mar**	**Advanced Buffer Overflow Attacks** By-passing non-executable stack Jumping to EAX, ESP, and EMP exploits	**Quiz 9** **Homework 1 due**
10 **29th Mar -** **4th Apr**	**Format String Vulnerabilities** Stack layout of variadic functions Exploit the format string	**Quiz 10**
11 **5th Apr -** **11th Apr**	**Linking** Load-time exploitation Basics of static and dynamic linking	**Quiz 11**
12 **12th Apr -** **18th Apr**		**Quiz 12** **Homework 2 released** **Homework 3 released**
13 **19th Apr -** **25th Apr**		**Quiz 13** **Homework 2 Due**

14 26th Apr – 2nd May		**Quiz 14**
15 3rd May - 9th May		**Homework 3 Due**

Note: This is a tentative schedule, and the instructor may add or remove lectures as necessary – 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.

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 04:00 PM the day before the assignment is due**. 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 will 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 will not receive feedback and will 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 will 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. Each assignment will contain more specific information regarding acceptable levels of collaboration.

						
Homework Assignments	✔	✔	✔	✔	✔	X

Quizzes	✔	✔	X	X	X	X
Final Exam	✔	✔	✔	✔	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

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. 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.
To view further information on the above, please visit the Office of Civil Rights and Sexual Misconduct's website at 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.