



MARYLAND APPLIED GRADUATE ENGINEERING

Embedded System Hacking and Security (ENPM664) Sections 0101 and CY01

Professors:

Mr. Robert Heinemann and Mr. Gananand Kini

Email: rlhr@umd.edu and gkini@umd.edu

Office Hours: TBD

Teaching Assistant: zelinlu@umd.edu

Email: Zelin Lu

Office Hours: TBD

Credits: 03

Term: Spring 2024

Course Dates: January 24th – May 9th

Course Times: Mondays 4:00 pm – 6:40 pm

Classroom: TBD and Online

Canvas/ELMS: <https://umd.instructure.com/courses/1339192>

Course Description

Computers pervade our everyday lives. However, desktops and laptops are just the tip of the iceberg representing just 2% of microprocessors produced. Hidden just beneath the surface is a substantial and diverse group of computers referred to as embedded systems. This massive category of machines represents 98% of processors produced today. This invisible but pervasive hardware underpins our society's most critical functions, which are being hacked. This course aims to reveal the tools, techniques, and procedures (TTPs) employed by adversaries to exploit and subvert the security of embedded systems.

This course will cover the core concepts and techniques to analyze and characterize the behavior of embedded systems and platforms. Concepts will be introduced and discussed within the context of an adversary intent on altering or subverting the behavior of such systems. The course does not expect students to have any prior embedded systems experience. After this course, the student will be familiar with: embedded system basics; basic soldering techniques; board analysis methodology; identification of peripherals, data buses, diagnostic ports, and tap points; device instrumentation; bus monitoring and decoding; development access via JTAG; Tools used for ARM assembly/disassembly; How shellcode is formatted; buffer overflow and/or return-oriented programming attacks; attacks similar to x86 platform.

Prerequisites

Prior programming experience, familiarity with computer architectures and reading assembly.

Learning Outcomes

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

- Define what an embedded system is and explain the basic architecture of an embedded system.
- Analyze a printed circuit board (PCB) and identify major components, peripherals, buses, diagnostic ports, and tap points.
- List the types of test equipment and tools used by hardware hackers and explain how they are used.
- Explain basic soldering techniques and specific PCB rework techniques used by hardware hackers.

- Instrument a printed circuit board (PCB) to monitor buses, decode data, and access diagnostic functionality.
- Identify software weaknesses in ARM-embedded architecture.
- Evaluate assembly code for exploits.
- Analyze and contrast exploitation techniques on RISC and CISC architectures.
- Apply exploitation techniques unique to ARM and embedded systems.
- Apply defenses to remediate ARM exploits.

Course Materials

- Course Hardware Kit (available through MAGE)
- Computer with Windows OS.
 - If you use Mac or Linux, have the ability to run a Windows Virtual Machine.
 - As a student, you qualify for a free windows license.
 - To get a windows license go to this link: <https://umd.onthehub.com/WebStore/Welcome.aspx>
 - Click on the start shopping button
 - Click the Windows 10 icon
 - Then click on add to cart
- VMWare Installed on Laptop (or VMWare Workstation Player)
- Etcher software installed on the laptop, <https://etcher.io/>
- Download a virtual machine and embedded system firmware image from https://drive.google.com/drive/folders/1SVwPN6rT_jhNGb5GoiwNOCQfnSPHjzFi?usp=share_link
 - There are two files named:
 - ESS_HWH_BBB_IMAGE_14JAN2018.img.xz
 - ESS_HWH_ESE_COMBINED_14JAN2018.zip

The laptop computer (not a notebook or a tablet!) should be capable of running a Linux virtual machine, have one free USB port, 30GB free on the hard disk.

Additionally, you will be required to use the course hardware kit starting the 2nd class meeting. The course hardware kit can be purchased from Maryland Applied Graduate Engineering (MAGE). Please see the below for information on purchasing and receiving the kits. NOTE: In the past, students have purchased kits from prior students. This is acceptable, but if any of the parts in the kit are broken, we will not be able to replace them.

How Much Is the Course Kit?

To be announced

Where Do I Pay?

<https://estore.eng.umd.edu/mage/enpm664-kit>

What Forms of Payment are Accepted?

Credit Card

Are the kits returnable/refundable?

No, the kits are a non-refundable purchase.

How do I get the kit?

On-Campus Sections

The kit will be delivered to your class on the first day only after your order is received via the website. **You need to have the kit by 2/5/24 to be able to move forward within the coursework properly.**

Online Sections

We will mail the kit to you. Please note that it can take up to a week to receive, depending on your location, so please plan your order date accordingly. **You need to have the kit by 2/5/24 to be able to move forward within the coursework properly.**

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 Monday 4:00 pm - 6:40 pm 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.

On-campus students come to class prepared to engage with the lecture and materials. 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. If you have a conflict on a particular day, please reach out to me in advance to discuss.

Communication Guidelines

Communicating with the Instructor

Our goal is to be readily available to you throughout the semester. We can be reached by email at rlhjr@umd.edu and gkini@umd.edu. Please DO NOT email us 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.

When constructing an email please put “ENPM 664: Your Topic” in the subject line. This will draw our attention to your email and enable us 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 an email asking for a meeting and we can set something up.

Announcements

We 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 %	Notes
Lab Reports	20%	Covers both Mr. Heinemann's and Mr. Kini's material
Homework	10%	Covers both Mr. Heinemann's and Mr. Kini's material
Quizzes	10%	Covers both Mr. Heinemann's and Mr. Kini's material
Midterm Exam	20%	Covers Mr. Heinemann's material
Final Exam	20%	Covers Mr. Kini's material
Final Project	20%	Project focused on hardware and/or software security of embedded systems
Total	100%	

Course Assignments

Lab Reports

- Each week there will be a practical exercise assigned. This will give the student a chance to practice hands-on the skills they learned in the lectures. The lab reports will consist of submitting writeups detailing their progression of the hands-on exercise.

Homework Assignments

- Homeworks will be assigned weekly. This will include reading assignments as well as questions pertaining to the week's lecture.

Quizzes

- There will be a short quiz each week. The quiz will consist of 3 - 5 questions and be 15 minutes in length. The purpose of the quiz is to test concepts that were introduced in the prior lecture. Quizzes are open notes.

Midterm Exam

- The Midterm will be administered using ELMS and will be taken online. There will not be a class meeting the week of the Midterm. The Midterm is open notes.

Final Project

- The team and its individual members research, demonstrate and present novel knowledge, analysis techniques and/or approaches to attacking OR defending embedded systems software (or both).
- The team and its individual members are able to demonstrate teamwork.
- The team and its individual members are able to plan, prioritize and execute tasks in order to achieve the outcome of the final project.
- The team and its individual members are able to analyze the security of the embedded system applying knowledge gained from the course and communicate the results of the analysis effectively.
- The team and its individual members demonstrate knowledge of embedded systems and the security of those systems.
- The teams with 4-5 members will be assigned to you by your Teaching Assistant (TA).

Final Exam

- The final will be administered using ELMS and will be taken online. The final will only include material from after the Midterm.

Grading of 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 2 weeks 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 ($89.99 \neq 90.00$). It would be unethical to make exceptions for some and not others.

Numerical course grades will be translated into letter grades as follows:

97 - 100	A+		60 - 77	C
90 - 96	A		50 - 59	D
87 - 89	B+		0 - 49	F
78 - 86	B			

Course Schedule

Week #	Date	Instructor	Weekly Description	Weekly Assignments	
1	1/29/24	Mr. Heinemann	Course Intro / Syllabus / Grading Course kit overview Lecture: What is ESS Lecture: Embedded Attack Tree Lecture: Embedded System Introduction	Reading Homework Final Project Assigned	
2	2/5/24	Mr. Heinemann	Quiz Lecture: Board Analysis Part 1 Lab: Getting to familiar with BBB	Reading Homework Lab Report	
3	2/12/2024	Mr. Heinemann	Quiz Lecture: Board Analysis Part 2 Lab: Board Analysis Lab	Reading Homework Lab Report	
4	2/19/24	Mr. Heinemann	Quiz Lecture: Embedded System Buses Lab: Monitoring & Decoding Buses Exercise Lecture: Soldering Technique	Reading Homework Lab Report	
5	2/26/24	Mr. Heinemann	Quiz Lecture: Development Access Lab: Development Access Exercise Lecture: Test Equipment & Tools	Reading Homework Lab Report	
6	3/4/24	Mr. Heinemann	Midterm Exam		
7	3/11/24	Mr. Kini	Lecture 1: Embedded Software Intro Lab: Linux Primer & Determining Beaglebone Black features	Final Project Proposal Draft	
8	3/18/24	Spring Break			
9	3/25/24	Mr. Kini	Homework and Lab Report Turn in Quiz Lecture 2: Bootloaders and Firmware Layouts Lab: U-Boot on the BBB and BBB Firmware analysis	Reading Homework Lab Report	

10	4/1/24	Mr. Kini	Homework and Lab Report Turn in Quiz Lecture 3: Firmware Analysis Lab: Extract Files from different firmwares	Reading Homework Lab Report Final Project Proposal
11	4/8/24	Mr. Kini	Homework and Lab Report Turn in Quiz Lecture 4: Instruction Set Architectures I Lab: Compile a program and reverse engineer it	Reading Homework Lab Report
12	4/15/24	Mr. Kini	Homework and Lab Report Turn in Quiz Lecture 5: Instruction Set Architectures II Lab: TBD	Reading Homework Lab Report
13	4/22/24	Mr. Kini	Homework and Lab Report Turn in Quiz Lecture 6: Binary Analysis Lab: TBD	Reading Homework Lab Report
14	4/29/24	Mr. Kini	Homework and Lab Report Turn in Quiz Lecture 7: Exploitation Lab: TBD	Reading Homework Lab Report
15	5/6/24	Mr. Kini	Final Homework and Lab Report Turn in Final Project Presentations/Demos Final Project Report, Presentation & Artifacts Due	Homework Lab Report Final Project Report, Presentations & Artifacts
16	5/13/24	Mr. Kini	Final Project Presentations and Final Exam	

Note: This is a tentative schedule, and subject to change 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 12:00 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.

	 OPEN NOTES	 USE BOOK	 LEARN ONLINE	 GATHER CONTENT With AI	 ASK FRIENDS	 WORK IN GROUPS
Lab Reports	✓	✓	✓	---	✓	---
Homework Assignments	✓	✓	✓	---	---	---
Quizzes	✓	✓	✓	---	---	---
Final Project	✓	✓	✓	✓	✓	✓
Midterm and Final Exams	✓	✓	---	---	---	---

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. 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 support 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.