Course Syllabus

695.744

T. McGuire

Johns Hopkins University

Instructor Contact

Tom McGuire
Cell: 443.267.8622
E-mail: tmcguir3@jhu.edu

I prefer that students contact me via email or through Microsoft Teams. Please be sure to include course number in the subject line. I will make every effort to respond to your inquiry within 24 hours or earlier. If an issue is urgent, please indicate "urgent" within the subject line of the email and I will respond as soon as is practical.

Office Hours via Zoom

This course will use Zoom to facilitate weekly, synchronous office hours. You are strongly encouraged to participate in Office Hours; you are responsible for ensuring that the material and information discussed during office hours is understood. You may find them very beneficial for receiving more timely answers to questions related to the course content and assignments.

Students will click the Office Hours link on the left menu to access Zoom and participate. You are encouraged to send any questions you would like to have answered during the live Office Hour sessions up to two (2) hours before the meeting. Recorded Office Hour sessions will be posted to the Office Hours Recordings area for any students who were unable to participate in the "live" sessions or for students who like to listen to them again.

For more information regarding Zoom, please see the Zoom Student Quick Start Guide.

Course Description

The course materials are divided into modules which can be accessed by clicking Course Modules on the left menu. A module will have several sections including the overview, content, readings, discussions, and assignments. You are encouraged to preview all sections of the module before starting. Most modules run for a period of seven (7) days, exceptions are noted in the Course Outline. You should regularly check Teams, the Calendar and Announcements for assignment due dates and any relevant changes. Please note that I make frequent announcements to help facilitate the class material.

Prerequisites

There are no formal prerequisites. It is highly recommended the student have some knowledge of Operating System Internals and C/Python programming experience.

Course Goals

To develop critical thinking skills required to analyze and protect against vulnerabilities in both source code and executable binaries. To analyze and detect malicious code running on systems. To better prepare students for the ever-evolving threat of vulnerabilities, exploits and malicious software in a real-world environment.

Course Objectives

By the end of the course, you will be able to:

- Identify and describe major programming errors and ways to mitigate the impact of discovered vulnerabilities.
- Analyze binary data and identify key characteristics and patterns of the data.
- Become proficient at debugging programs, identifying misbehaving code, and understanding ways vulnerabilities can be exploited.
- Identify key characteristics of malware and ways to mitigate the threat of malware.

Course Structure

The course materials are divided into modules which can be accessed by clicking **Course Modules** on the left menu. A module will have several sections including the overview, content, readings, discussions, and assignments. You are encouraged to preview all sections of the module before starting. Most modules run for a period of seven (7) days, exceptions are noted in the **Course Outline**. You should regularly check the **Calendar** and **Announcements** for assignment due dates.

Textbook

Textbook information for this course is available online through the appropriate bookstore website: For online courses, search the MBS website.

Recommended

- Dowd, M., McDonald, J., & Schuh, J. (2007). The art of software security assessment identifying and preventing software vulnerabilities. Addison-Wesley.

  ISBN-10: 0-321-44442-6

  ISBN-13: 978-0-321-44442-4

Optional

- Eagle, C. (2008). The IDA Pro book. No Starch Press.

  ISBN-10: 1-59327-289-8

  ISBN-13: 978-1-59327-289-0

- Sikorski, M. (2012). Practical malware analysis. No Starch Press.

  ISBN-10: 1-59327-290-1

  ISBN-13: 978-1-59327-290-6

- Eilam, E. (2013). Reversing: secrets of reverse engineering. Wiley.

  ISBN-10: 0-76457-481-7

  ISBN-13: 978-0-76457-481-8

- Dang, B., Gazet, A., & Bachaalany, E. (2014). Practical reverse engineering: x86, x64, Arm, Windows Kernel, reversing tools, and obfuscation. Wiley.

  ISBN-10: 1-11878-731-5

  ISBN-13: 978-1-11878-731-1

Other

Refer to the bottom of the Course Outline for other resources that you may find helpful throughout the course.

Required Software

You will have access to "D2L Learning" and "Microsoft Azure Tools" accounts which provide the ability to download the software listed below. **You will not need to purchase any software, as your course fee covers the cost of these accounts and software. Instructions for creating these accounts can be found within the first module**. If you have any questions regarding which software to download or install, or how to install it, please don't hesitate to ask.

This course heavily relies on running virtual machines in order to provide a safe sandbox for performing malware analysis. There are many additional pieces of software which will be installed within your virtual machine environments, please see the VM Environments PDF, located in Blackboard, for further information (including links to the software). In addition, be sure to check Blackboard frequently for the most up-to-date information as software installation instructions or operating system settings may change over time.

VMWare Workstation/Fusion

You will need access to virtualization software, and I recommend you use these as they are the industry standard (VMWare Workstation for Windows and Linux, and VMWare Fusion for macOS). A license for each is provided at no cost to you and details for obtaining the license key are provided in the first module. Course materials, such as setup guides and configuration, have been written assuming one of these products is being used. If you are more comfortable with an alternative (e.g. VirtualBox, qemu), you are free to use it with the understanding that you may run into issues since I have not tested the integration of course materials with all virtualization products.

Microsoft Windows

You will need a virtual machine running Microsoft Windows. A license for this is provided at no cost to you and details for obtaining the license key are provided in the first module. Specific software packages that should be installed within the virtual machine can be found in the VM Environments PDF.

Ubuntu Linux

You will need a virtual machine running the Ubuntu distribution of Linux. This operating system is free and does not require a license - a link to where it can be obtained will be provided in the first module. Specific software packages that should be installed within the virtual machine can be found in the VM Environments PDF.

Student Coursework Requirements

It is expected that each module will take approximately 7-10 hours per week to complete. Here is an approximate breakdown: reading the assigned sections of the texts (approximately 3-4 hours per week) as well as some outside reading, listening to the audio annotated slide presentations (approximately 2-3 hours per week), and writing assignments (approximately 2-3 hours per week).

All file submissions should include your JHED ID in the filename, unless otherwise noted in the assignment. Late submissions will receive point deductions unless otherwise coordinated with the instructors. Coordination of late submissions must be done prior to the due date; however, I understand that unforeseen circumstances do occur. Please reach out as early as you can.

This course will consist of the following basic student requirements:

Preparation and Participation (15% of Final Grade Calculation)

You are responsible for carefully reading all assigned material and being prepared for discussion. The majority of readings are from the course text. Additional reading may be assigned to supplement text readings.

Post your initial response to the discussion questions by the Thursday evening for that module week. Posting an initial response to the discussion question is part one of your grade for module discussions (i.e., Timeliness).

Part two of your grade for module discussion is your interaction (i.e., responding to classmate postings with thoughtful responses) with **at least two (2)** classmates (i.e., Critical Thinking). Just posting your response to a discussion question is not sufficient; I want you to interact with your classmates. Be detailed in your postings and in your responses to your classmates' postings. Feel free to agree or disagree with your classmates. Please ensure that your postings are civil and constructive.

I will monitor module discussions and will respond to some of the discussions as discussions are posted. **You are responsible for responding to questions raised by me or fellow students within any threads you participate in. Keep in mind, all discussion content is part of the course and thus may appear on exams**.

All prompts will require some research to be done, and the expectation is the sources that are utilized are properly cited.

Evaluation of preparation and participation is based on contribution to discussions.

Preparation and participation is evaluated by the following grading elements:

- Timeliness (50%)
- Critical Thinking (50%)

Preparation and participation is graded as follows:

- 100-90 = A - Timeliness [regularly participates; all required postings; early in discussion; throughout the discussion]; Critical Thinking [rich in content; full of thoughts, insight, and analysis].
- 89-80 = B - Timeliness [frequently participates; all required postings; some not in time for others to read and respond]; Critical Thinking [substantial information; thought, insight, and analysis has taken place].
- 79-70 = C - Timeliness [infrequently participates; all required postings; most at the last minute without allowing for response time]; Critical Thinking [generally competent; information is thin and commonplace].
- <70 = F - Timeliness [rarely participates; some, or all required postings missing]; Critical Thinking [rudimentary and superficial; no analysis or insight is displayed].

Self Assessments (5% of Final Grade Calculation)

Most modules will have a self-assessment. You may take these self-assessments as many times as you'd like, however, only the first score will be counted towards your self-assessment totals.

These assessments are there to help you make sure you are on track for understanding the material each week.

Assignments (20% of Final Grade Calculation)

Assignments will include a mix of qualitative assignments (e.g. literature reviews, model summaries), quantitative problem sets, and case study updates. Include your name and JHED ID within the assignment itself, either on a cover page or within a header/footer. All Figures and Tables should be captioned and labeled appropriately.

All assignments are due according to the dates in the Calendar or Course Outline.

Late submissions will be deducted 10 points each day the assignment is late. Submissions beyond 3 days will receive a 0 unless otherwise coordinated with the instructor..

If, after submitting a written assignment you are not satisfied with the grade received, you are encouraged to reach out to the instructor(s) to discuss the deductions. Allowing resubmission for partial credit will be determined on a case-by-case basis.

Qualitative assignments are evaluated by the following grading elements:

- Each part of question is answered (20%)
- Writing quality and technical accuracy (30%) (Writing is expected to meet or exceed accepted graduate-level English and scholarship standards. That is, all assignments will be graded on grammar and style as well as content.)
- Rationale for answer is provided (20%)
- Examples are included to illustrate rationale (15%) (If you do not have direct experience related to a particular question, then you are to provide analogies versus examples.)

- Outside references are included (15%)

Qualitative assignments are graded as follows:

- 100-90 = A - All parts of question are addressed; Writing Quality/ Rationale/Examples/Outside References [rich in content; full of thought, insight, and analysis].
- 89-80 = B - All parts of the question are addressed; Writing Quality/ Rationale/Examples/Outside References [substantial information; thought, insight, and analysis has taken place].
- 79-70= C - Majority of parts of the question are addressed; Writing Quality/Rationale/Examples/Outside References [generally competent; information is thin and commonplace].
- <70 = F - Some parts of the question are addressed; Writing Quality/Rationale/Examples/Outside References [rudimentary and superficial; no analysis or insight displayed].

Quantitative assignments are evaluated by the following grading elements:

- Each part of question is answered (20%)
- Assumptions are clearly stated (20%)
- Intermediate derivations and calculations are provided (25%)
- Answer is technically correct and is clearly indicated (25%)
- Answer precision and units are appropriate (10%)

Quantitative assignments are graded as follows:

- 100-90 = A - All parts of question are addressed; All assumptions are clearly stated; All intermediate derivations and calculations are provided; Answer is technically correct and is clearly indicated; Answer precision and units are appropriate.
- 89-80 = B - All parts of question are addressed; All assumptions are clearly stated; Some intermediate derivations and calculations are provided; Answer is technically correct and is indicated; Answer precision and units are appropriate.
- 79-70 = C - Most parts of question are addressed; Assumptions are partially stated; Few intermediate derivations and calculations are provided; Answer is not technically correct but is indicated; Answer precision and units are indicated but inappropriate.
- <70 = F - Some parts of the question are addressed; Assumptions are not stated; Intermediate derivations and calculations are not provided; The answer is incorrect or missing; The answer precision and units are inappropriate or missing.

Course Project (30% of Final Grade Calculation)

There will be two (2) course projects assigned throughout the course.

Late projects will be deducted 15 points each day the project is late.

The course projects are evaluated by the following grading elements:

- Student preparation and participation (as described in Course Project Description) (40%)
- Student technical understanding of the course project topic (as related to individual role that the student assumes and described in the Course Project Description) (20%)
- Team preparation and participation (as described in Course Project Description) (20%)
- Team technical understanding of the course project topic (as related to the Customer Team roles assumed by the students and the Seller Team roles assumed by the students and described in the Course Project Description) (20%)

Course Projects are graded as follows:

- 100-90 = A - Student Preparation and Participation/Team Preparation and Participation [individual/team roles and responsibilities well defined and understood; individual/team well versed in use of video conferencing software; individual/team work product(s) agreed to, well prepared and available to all team members/instructors]; Student Understanding/Team Understanding [rich in content; full of thought, insight, and analysis].
- 89-80 = B - Student Preparation and Participation/Team Preparation and Participation [individual/team roles and responsibilities well defined and understood; individual/team well versed in use of Adobe Connect; individual/team work product(s) agreed to and prepared]; Student Understanding/Team Understanding [substantial information; thought, insight, and analysis has taken place].
- 79-70 = C - Student Preparation and Participation/Team Preparation and Participation [individual/team roles and responsibilities agreed to; individual/team well versed in use of Adobe Connect; individual/ team work product(s) prepared]; Student Understanding/Team Understanding [generally competent; information is thin and commonplace].
- <70 = F - Student Preparation and Participation/Team Preparation and Participation [individual/team roles and responsibilities not well understood; individual/team has difficult with use of Adobe Connect; individual/team work product(s) partially prepared]; Student Understanding/Team Understanding [rudimentary and superficial; no analysis or insight displayed].

Exams (30% of Final Grade Calculation, combined from 15% for Midterm and 15% for Final)

The midterm exam will be available around Module 7 and the final exam will be available in the next-to-last Module. You will have one week to complete the exams and they will be due by 11:59 PM exactly one week from their release. You may use the course text and any notes to complete the exams.

Late submission of exams are not accepted without prior coordination. Failure to cite sources will result in a full letter grade reduction.

The exams are evaluated by the following grading elements:

- Each part of question is answered (20%)
- Writing quality and technical accuracy (30%) (Writing is expected to meet or exceed accepted graduate-level English and scholarship standards. That is, all assignments will be graded on grammar and style as well as content.)
- Rationale for answer is provided (20%)
- Examples are included to illustrate rationale (15%) (If a student does not have direct experience related to a particular question, then the student is to provide analogies versus examples.)
- Outside references are included (15%)

Exams are graded as follows:

- 100-90 = A - All parts of question are addressed; Writing Quality/ Rationale/Examples/Outside References [rich in content; full of thought, insight, and analysis].
- 89-80 = B - All parts of the question are addressed; Writing Quality/ Rationale/Examples/Outside References [substantial information; thought, insight, and analysis has taken place].
- 79-70 = C - Majority of parts of the question are addressed; Writing Quality/Rationale/Examples/Outside References [generally competent; information is thin and commonplace].
- <70 = F - Some parts of the question are addressed; Writing Quality/Rationale/Examples/Outside References [rudimentary and superficial; no analysis or insight displayed].

Grading

Assignments are due according to the dates posted in the Blackboard course site. You may check these due dates in the Course Calendar or the Assignments in the corresponding modules. I will post grades within the week after assignment due dates.

I generally do not directly grade spelling and grammar. However, egregious violations of the rules of the English language will be noted without comment. Consistently poor performance in either spelling or grammar is taken as an indication of poor written communication ability that may detract from your grade.

A grade of A indicates achievement of consistent excellence and distinction throughout the course - that is, conspicuous excellence in all aspects of assignments and discussion in every week.

A grade of B indicates work that meets all course requirements on a level appropriate for graduate academic work. These criteria apply to both undergraduates and graduate students taking the course.

100-94 = A

93-90 = A-

89-87 = B+

86-83 = B

82-80 = B-

79-70 = C

<63 = F

Final grades will be determined by the following weighting:

Item	**% of Grade**
Preparation and Participation	15%
Self Assessments	5%
Assignments	20%
Course Projects	30% (15% + 15%)
Exams (Midterm + Final)	30% (15% + 15%)

Help & Support

You should refer to **Help & Support** on the left menu for a listing of all the student services and support available.

Policies and Guidelines

Academic Integrity

Academic Misconduct Policy

All students are required to read, know, and comply with the Johns Hopkins University Krieger School of Arts and Sciences (KSAS)/Whiting School of Engineering (WSE) Procedures for Handling Allegations of Misconduct by Full-Time and Part-Time Graduate Students.

This policy prohibits academic misconduct, including but not limited to the following: cheating or facilitating cheating; plagiarism; reuse of assignments; unauthorized collaboration; alteration of graded assignments; and unfair competition. You may request a paper copy of this policy at this by contacting jhep@jhu.edu.

Policy on Disability Services

Johns Hopkins University (JHU) is committed to creating a welcoming and inclusive environment for students, faculty, staff and visitors with disabilities. The University does not discriminate on the basis of race, color, sex, religion, sexual orientation, national or ethnic origin, age, disability or veteran status in any student program or activity, or with regard to admission or employment. JHU works to ensure that students, employees and visitors with disabilities have equal access to university programs, facilities, technology and websites.

Under Section 504 of the Rehabilitation Act of 1973, the Americans with Disabilities Act (ADA) of 1990 and the ADA Amendments Act of 2008, a person is considered to have a disability if c (1) he or she has a physical or mental impairment that substantially limits one or more major life activities (such as hearing, seeing, speaking, breathing, performing manual tasks, walking, caring for oneself, learning, or concentrating); (2) has a record of having such an impairment; or (3) is regarded as having such an impairment class. The University provides reasonable and appropriate accommodations to students and employees with disabilities. In most cases, JHU will require documentation of the disability and the need for the specific requested accommodation.

The Disability Services program within the Office of Institutional Equity oversees the coordination of reasonable accommodations for students and employees with disabilities, and serves as the central point of contact for information on physical and programmatic access at the University. More information on this policy may be found at the Disabilities Services website or by contacting (410) 516-8075.

Disability Services

Johns Hopkins Engineering for Professionals is committed to providing reasonable and appropriate accommodations to students with disabilities.

Students requiring accommodations are encouraged to contact Disability Services at least four weeks before the start of the academic term or as soon as possible. Although requests can be made at any time, students should understand that there may be a delay of up to two weeks for implementation depending on the nature of the accommodations requested.

Requesting Accommodation

New students must submit a Disability Services Graduate Registration Form along with supporting documentation from a qualified diagnostician that:

- Identifies the type of disability
- Describes the current level of functioning in an academic setting
- Lists recommended accommodations

Questions about disability resources and requests for accommodation at Johns Hopkins Engineering for Professionals should be directed to:

EP Disability Services
Phone: 410-516-2306
Fax: 410-579-8049
E-mail: ep-disability-svcs@jhu.edu