MET CS 763 Secure Software Development
2026 Fall 2 Online Course Syllabus

Instructor

Yuting Zhang, Ph.D. danazh@bu.edu

Course Duration

Start: October 27, 2026
End: December 14, 2026

Course credits

4 credits

Course Description

Overview of techniques and tools to develop secure software. Focus on application security. Topics include secure software development processes, DevSecOps, threat modeling, secure requirements and architectures, vulnerability and malware analysis using static code analysis and dynamic analysis tools, vulnerabilities in C/C++ and Java programs, Crypto and secure APIs, vulnerabilities in web applications and mobile applications and security testing. Hands-on lab and programming exercises using current tools are provided and required. 4 credits.

Course Learning Objectives

By successfully completing this course, you will be able to do the following:

- Explain secure software development process and activities in the process.
- Explain security principles and how to apply them in software development.
- Explain risk management and threat modeling and identify security requirements and threats in real world projects.
- Explain, identify and apply DevSecOps best practices in real world applications
- Explain and identify common vulnerabilities and corresponding mitigations in programs written in high-level programming languages such as C/C++. Java, Python.
- Explain basic cryptographic algorithms and implement security features with proper crypto APIs in the application.
- Explain the security mechanisms and identify common vulnerabilities and corresponding mitigations in web applications and mobile applications.
- Design and conduct security testing for real world applications.
- Apply AI-assisted tools to enhance security and evaluate their strength

Course Materials

Required Book

There are no required textbooks, but some reference books, and additional reading materials will also be provided in class.

Reference Books

Du, W. (2022). Computer Security: A Hands-on Approach (3rd ed.). Independently Published. ISBN 9781733003957.

McGraw, G. (2006). Software Security: Building Security In. Addison-Wesley Professional. ISBN 9780321356703.

Howard, M., LeBlanc, D., & Viega, J. (2009). 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. McGraw-Hill Education. ISBN 9780071626750.
An e-book is available at Vitalsource.com. An e-book is available through Amazon.

Additional Books

- Ross Anderson. Security Engineering. Wiley. 2nd Edition.
- Mathias Paye. Software Security Principles, Policies, and Protection. (January 2019, v0.33)
- Theodor Richardson & Charles Thies. Secure Software Design. Jones & Bartlett Learning.
- 2013
- Dafydd Stuttard & Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition. Wiley.

Other Reading Materials

- Microsoft Secure Development Life Cycle
- OWASP SAMM Project
- OWASP TOP 10
- Developer Guide
- Testing Guide
- Secure Coding Practice Guideline
- Seed Labs

Study Guide and Timeline of Deliverables

Module 1 Study Guide and Deliverables (October 27 – November 2, 2026)

Module Theme: Introduction to Secure Software Development Process and DevOps

Readings:

- Related chapters in the reference books. Additional reading materials required in the lecture notes.

Discussions:

- Module 1 Discussion posts due by **Tuesday, November 3 at 6:00 am ET**

Assignments:

- Project Assignment 1 due on **Tuesday, November 3 at 6:00 am ET**
- Begin work on Lab 1

Assessments:

- No Assessments this module

Live Classrooms:

- **Wednesday, October 28 from 7:00-9:00 pm ET**
- **Saturday, October 31 from 7:00-8:00 pm ET**

Module 2 Study Guide and Deliverables
(November 3 – November 9, 2026)

Module Theme: Security Principles and Design

Readings:

- Related chapters in the reference books. Additional reading materials required in the lecture notes.

Discussions:

- Module 2 Discussion posts due on **Tuesday, November 10 at 6:00 am ET**

Assignments:

- Lab 1 due on **Tuesday, November 10 at 6:00 am ET**
- Begin work on Project Assignment 2

Assessments:

- Quiz 1 due on **Tuesday, November 10 at 6:00 am ET**

Live Classrooms:

- **Wednesday, November 4 from 7:00-9:00 pm ET**
- **Saturday, November 7 from 7:00-8:00 pm ET**

Module 3 Study Guide and Deliverables
(November 10 – November 16, 2026)

Module Theme: Secure Coding and Language Level Vulnerabilities

Readings:

- Related chapters in the reference books. Additional reading materials required in the lecture notes.

Discussions:

- Module 3 Discussion posts due on **Tuesday, November 17 at 6:00 am ET**

Assignments:

- Project Assignment 2 due on **Tuesday, November 17 at 6:00 am ET**
- Begin work on Lab 2

Assessments:

No Assessments in this module

Live Classrooms:

- **Wednesday, November 11 from 7:00-9:00 pm ET**
- **Saturday, November 14 from 7:00-8:00 pm ET**

Module 4 Study Guide and Deliverables
(November 17 – November 23, 2026)

Module Theme: Crypto Basics and Sins

Readings:

- Related chapters in the reference books. Additional reading materials required in the lecture notes.

Discussions:

- No discussion questions this week.

Assignments:

- Lab 2 due on **Tuesday, November 24 at 6:00 am ET**
- Begin work on Project Assignment 3

Assessments:

- Quiz 2 due on **Tuesday, November 24 at 6:00 am ET**

Live Classrooms:

- **Wednesday, November 18 from 7:00-9:00 pm ET**
- **Saturday, November 21 from 7:00-8:00 pm ET**

Module 5 Study Guide and Deliverables (November 24 – November 30, 2026)

Module Theme: Web Application Security

Readings:

- Related chapters in the reference books. Additional reading materials required in the lecture notes.

Discussions:

- Module 5 Discussion posts due on **Tuesday, December 1 at 6:00 am ET**

Assignments:

- Project Assignment 3 due on **Tuesday, December 1 at 6:00 am ET**
- Lab 3 due on **Tuesday, December 1 at 6:00 am ET**

Assessments:

- No Assessments this module

Live Classrooms:

- **Wednesday, November 25 from 7:00-9:00 pm ET**
- **Saturday, November 28 from 7:00-8:00 pm ET**

Module 6 Study Guide and Deliverables (December 1 – December 7, 2026)

Module Theme: Mobile Security and Security Testing Reverse Engineering?

Readings:

- Related chapters in the reference books. Additional reading materials required in the lecture notes.

Discussions:

- Module 6 Discussion posts due on **Tuesday, December 8 at 6:00 am ET**

Assignments:

- Project Assignment 4 due on **Tuesday, December 8 at 6:00 am ET**

Assessments:

- Quiz 3 due on **Tuesday, December 8 at 6:00 am ET**

Live Classrooms:

- **Wednesday, December 2 from 7:00-9:00 pm ET**
- **Saturday, December 5 from 7:00-8:00 pm ET**

Course Evaluation:

Please complete the course evaluation once you receive an email or Blackboard notification indicating the evaluation is open. Your feedback is important to MET, as it helps us make improvements to the program and the course for future students.

Final Exam Details

The Final Exam is a proctored exam available from **Wednesday, December 9, 2026, at 6:00 AM ET to Saturday, December 12, 2026, at 11:59 PM ET**.

The Computer Science department requires that all final exams be administered using an online proctoring service, which you will access via your course in Blackboard. In order to take the exam, you are required to have a working computer, webcam, speakers, and microphone that meet the proctoring service's system requirements. A detailed list of those requirements can be found in the Proctored Exam Information module located on the course home page. Additional information regarding your proctored exam will be forthcoming from the Assessment Administrator.

The exam is accessible during the final exam period. You can access it from the Assessments section of the course. Your proctor will enter the password to start the exam.

Final Exam Duration: **three hours (180 minutes)**

You will receive a technical support hotline number before the start of the exam. Please bring this number with you to the exam.

Evaluation of Students and Grading

Grading Policy

The grade that a student receives in this class will be based on class participation, in-class exercises, lab assignments, project assignments, quizzes, and the final exam. The grade is broken down as shown below. All percentages are approximate and the instructor reserves the right to make necessary changes.

Deliverable	**Weight**
Discussion Participation	5%
Lab Assignments	25%
Project Assignments	30%
Quizzes	10%
Final Exam	30%

Letter grade/numerical grade conversion is shown below:

Letter Grade	**Approximate Grade Range by Percentage**
A	95–100
A–	90–94
B+	85–89
B	80–84
B–	77-79
C+	74-76
C	70-73
C–	65-70
D	60–65

F	0–59

Discussion Participation

There is a total of 5 module discussions: They include 3 discussion questions and 2 project information sharing prompts.

For each discussion forum, each student should start a new thread to post an original message and reply to at least one other student's message.

This forum is graded as follows:

- Your own post - 75%
- Reply to at least one another post - 25%

Module discussions are accessed from within the course module or at the Discussions top tab.

Lab Assignments

There is a total of 3 lab assignments. Lab 1 is to introduce students to use some SAST tools. Lab 2 is to introduce students how to attack and defeat buffer overflow attacks. This lab requires some basic knowledge about C programming and memory layout, which will be discussed in the Module 3. Lab 3 is to introduce students to web security, how to launch and defeat XSS attacks. This lab requires some basic knowledge about Javascript.

Lab Assignments are accessed from the Assignments link in the left-side navigation menu.

Project Assignments

The project assignment is split into 4 assignments. Project Assignment 1 is the project proposal. Students need to choose a project and set up a github repository for it. Project Assignment 2 requires students elicit and analyze the security requirements of the chosen projects, identify some new security requirements, as well as perform risk analysis of the software architecture, such as performing a threat modeling. Project Assignment 3 requires students to implement new security features using cryptography APIs into the existing project. Project Assignment 4 requires students to run some security tools such as SAST and DAST tools on the project and analyze the results.

Project Assignments are accessed from the Assignments link in the left-side navigation menu.

Quizzes

There will be 3 quizzes throughout the course to assess the information presented in the module lecture notes.

Quizzes are accessed from within the corresponding module.

Attendance Policy

Attendance is expected at all class meetings. You are responsible for all materials discussed in class. In general, no makeup quizzes and exams will be given unless an extremely good, verifiable reason is given in advance.

Assignment Late Policy

Every assignment has a due date. Late assignments submitted within three days after the deadline will be penalized. *No assignments will be accepted 3 days after the deadline.* It is the students' responsibility to keep secure backups of all assignments.

Course Policies and Academic Conduct

Please visit Metropolitan College's website for the full text of the department's *Academic Conduct Code*

Policy for the Use of Generative AI

Please read carefully the general AI guidelines for BU students at https://www.bu.edu/aida/guidance/generative-ai-guidelines-for-students/.

In this course, students are encouraged to use AI tools to enhance learning, research, and productivity. In particular, students are recommended to use AI tools as part of the secure software development process in course projects to improve software security.

However, students must independently develop and demonstrate their own technical skills, critical thinking, and academic integrity. AI tools are intended to assist, not replace student learning and problem-solving.

Students are prohibited from:

- Submitting AI-generated assignments (e.g., lab reports, discussion posts, project reports, or other written work) as if they were entirely their own work.

- Relying on AI-generated outputs without reviewing, verifying, testing, and understanding the results.
- Using AI tools in ways that violate academic integrity policies or misrepresent authorship.

For every assignment, students must include an AI Usage Disclosure describing whether AI tools were used and, if so, how they were used. Specific disclosure requirements will be provided in each assignment description

A Definition of Plagiarism

> "The academic counterpart of the bank embezzler and of the manufacturer who mislabels products is the plagiarist: the student or scholar who leads readers to believe that what they are reading is the original work of the writer when it is not. If it could be assumed that the distinction between plagiarism and honest use of sources is perfectly clear in everyone's mind, there would be no need for the explanation that follows; merely the warning with which this definition concludes would be enough. But it is apparent that sometimes people of goodwill draw the suspicion of guilt upon themselves (and, indeed, are guilty) simply because they are not aware of the illegitimacy of certain kinds of "borrowing" and of the procedures for correct identification of materials other than those gained through independent research and reflection."
>
> "The spectrum is a wide one. At one end there is a word-for-word copying of another's writing without enclosing the copied passage in quotation marks and identifying it in a footnote, both of which are necessary. (This includes, of course, the copying of all or any part of another student's paper.) It hardly seems possible that anyone of college age or more could do that without clear intent to deceive. At the other end there is the almost casual slipping in of a particularly apt term which one has come across in reading and which so aptly expresses one's opinion that one is tempted to make it personal property."
>
> "Between these poles there are degrees and degrees, but they may be roughly placed in two groups. Close to outright and blatant deceit-but more the result, perhaps, of laziness than of bad intent-is the patching together of random jottings made in the course of reading, generally without careful identification of their source, and then woven into the text, so that the result is a mosaic of other people's ideas and words, the writer's sole contribution being the cement to hold the pieces together. Indicative of more effort and, for that reason, somewhat closer to honest, though still dishonest, is the paraphrase, and abbreviated (and often skillfully prepared) restatement of someone else's analysis or conclusion, without acknowledgment that another person's text has been the basis for the recapitulation."

The paragraphs above are from H. Martin and R. Ohmann, The Logic and Rhetoric of Exposition, Revised Edition. Copyright 1963, Holt, Rinehart and Winston.

Academic Conduct Code

I. Philosophy of Discipline

The objective of Boston University in enforcing academic rules is to promote a community atmosphere in which learning can best take place. Such an atmosphere can be maintained only so long as every student believes that his or her academic competence is being judged fairly and that he or she will not be put at a disadvantage because of someone else's dishonesty. Penalties should be carefully determined so as to be no more and no less than required to maintain the desired atmosphere. In defining violations of this code, the intent is to protect the integrity of the educational process.

II. Academic Misconduct

Academic misconduct is conduct by which a student misrepresents his or her academic accomplishments, or impedes other students' opportunities of being judged fairly for their academic work. Knowingly allowing others to represent your work as their own is as serious an offense as submitting another's work as your own.

III. Violations of this Code

Violations of this code comprise attempts to be dishonest or deceptive in the performance of academic work in or out of the classroom, alterations of academic records, alterations of official data on paper or electronic resumes, or unauthorized collaboration with another student or students. Violations include, but are not limited to:

A. **Cheating on examination**. Any attempt by a student to alter his or her performance on an examination in violation of that examination's stated or commonly understood ground rules.

B. **Plagiarism.** Representing the work of another as one's own. Plagiarism includes but is not limited to the following: copying the answers of another student on an examination, copying or restating the work or ideas of another person or persons in any oral or written work (printed or electronic) without citing the appropriate source, and collaborating with someone else in an academic endeavor without acknowledging his or her contribution. Plagiarism can consist of acts of commission-appropriating the words or ideas of another-or omission failing to acknowledge/document/credit the source or creator of words or ideas (see below for a detailed definition of plagiarism). It also includes colluding with someone else in an academic endeavor without acknowledging his or her contribution, using audio or video footage that comes from another source (including work done by another student) without permission and acknowledgement of that source.

C. **Misrepresentation or falsification of data** presented for surveys, experiments, reports, etc., which includes but is not limited to: citing authors that do not exist;

citing interviews that never took place, or field work that was not completed.

D. **Theft of an examination**. Stealing or otherwise discovering and/or making known to others the contents of an examination that has not yet been administered.

E. **Unauthorized communication during examinations**. Any unauthorized communication may be considered prima facie evidence of cheating.

F. **Knowingly allowing another student to represent your work as his or her own**. This includes providing a copy of your paper or laboratory report to another student without the explicit permission of the instructor(s).

G. **Forgery, alteration, or knowing misuse of graded examinations, quizzes, grade lists, or official records of documents**, including but not limited to transcripts from any institution, letters of recommendation, degree certificates, examinations, quizzes, or other work after submission.

H. **Theft or destruction of examinations or papers** after submission.

I. **Submitting the same work in more than one course** without the consent of instructors.

J. **Altering or destroying another student's work or records**, altering records of any kind, removing materials from libraries or offices without consent, or in any way interfering with the work of others so as to impede their academic performance.

K. **Violation of the rules governing teamwork**. Unless the instructor of a course otherwise specifically provides instructions to the contrary, the following rules apply to teamwork: 1. No team member shall intentionally restrict or inhibit another team member's access to team meetings, team work-in-progress, or other team activities without the express authorization of the instructor. 2. All team members shall be held responsible for the content of all teamwork submitted for evaluation as if each team member had individually submitted the entire work product of their team as their own work.

L. **Failure to sit in a specifically assigned seat during examinations.**

M. **Conduct in a professional field assignment that violates the policies and regulations of the host school or agency.**

N. **Conduct in violation of public law occurring outside the University that directly affects the academic and professional status of the student, after civil authorities have imposed sanctions.**

O. **Attempting improperly to influence the award of any credit, grade, or honor.**

P. **Intentionally making false statements to the Academic Conduct Committee or intentionally presenting false information to the Committee.**

Q. **Failure to comply with the sanctions imposed under the authority of this code.**

Important Message on Final Exams

Dear Boston University Computer Science Online Student,

As part of our ongoing efforts to maintain the high academic standard of all Boston University programs, including our online MSCIS degree program, the Computer Science Department at Boston University's Metropolitan College requires that each of the online courses includes a proctored final examination.

By requiring proctored finals, we are ensuring the excellence and fairness of our program. The final exam is administered online.

Specific information regarding final-exam scheduling will be provided approximately two weeks into the course. This early notification is being given so that you will have enough time to plan for where you will take the final exam.

I know that you recognize the value of your Boston University degree and that you will support the efforts of the University to maintain the highest standards in our online degree program.

Thank you very much for your support with this important issue.

Regards,

Professor Lou Chitkushev, Ph.D.

Associate Dean for Academic Affairs

Boston University Metropolitan College

Who's Who: Roles and Responsibilities

You will meet many BU people in this course and program. Some of these people you will meet online, and some you will communicate with by email and telephone. There are many people behind the scenes, too, including instructional designers, faculty who assist with course preparation, and video and animation specialists.

People in Your Online Course in Addition to Your Fellow Students

Your Facilitator. Our classes are divided into small groups, and each group has its own facilitator. We carefully select and train our facilitators for their expertise in the subject matter and their excellence in teaching. Your facilitator is responsible for stimulating discussions in pedagogically useful areas, for answering your questions, and for grading homework assignments, discussions, term projects, and any manually graded quiz or final-

exam questions. If you ask your facilitator a question by email, you should get a response within 24 hours, and usually faster. If you need a question answered urgently, post your question to one of the urgent help topics, where everyone can see it and answer it.

Your Professor. The professor for your course has primary responsibility for the course. If you have any questions that your facilitator doesn't answer quickly and to your satisfaction, then send your professor an email in the course, with a cc to your facilitator so that your facilitator is aware of your question and your professor's response.

Your Lead Faculty and Student Support Administrator, Jennifer Sullivan. Jen is here to ensure you have a positive online experience. You will receive emails and announcements from Jen throughout the semester. Jen represents Boston University's university services and works for BU Virtual. She prepares students for milestones such as course launch, final exams, and course evaluations. She is a resource to both students and faculty. For example, Jen can direct your university questions and concerns to the appropriate party. She also handles general questions regarding Online Campus functionality for students, faculty, and facilitators, but she does not provide tech support. She is enrolled in all classes and can be contacted within the course through Online Campus email as it is running. You can also contact her by external email at jensul@bu.edu .

Disability and Access Services

In accordance with university policy, every effort will be made to accommodate students with respect to speech, hearing, vision, or other disabilities. Any student who may need an accommodation for a documented disability should contact Disability and Access Services at 617-353-3658 or at access@bu.edu for review and approval of accommodation requests.

Once a student receives their accommodation letter, they must send it to their instructor and/or facilitator each semester. They must also send a copy to their Faculty & Student Support Administrator, who may need to update the course settings to ensure accommodation is in place. Accommodation cannot be implemented if the students do not send their letters.