CS 763 Secure Software Development

Department of Computer Science

Metropolitan College

Boston University

Spring 2022 Syllabus

Instructor Information

Name: Yuting Zhang
Office: 1010 Commonwealth ave, Rm 322
Email: danazh at bu dot edu
URL: http://people.bu.edu/danazh

Course Information

Lecture time and location

Monday 6:00-8:45, PSY B39

Prerequisites

At least two 500- level (or above) computer programming-intensive science courses or instructor's consent. As this is an advanced 700 level course, you should be familiar with programming and software development.

Reference Books:

Wenliang Du, Computer & Internet Security: A Hands-on Approach 2nd Edition. May 1, 2019.

Gary McGraw. Software Security: Building Security In. Addison-Wesley Professional; 1 edition (February 2, 2006)

Michael Howard, David LeBlanc & John Viega . 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (Networking & Comm - OMG). McGraw-Hill Education; 1 edition (September 24, 2009)

Additional Books:

Ross Anderson. Security Engineering. Wiley. 2 edition. (https://www.cl.cam.ac.uk/~rja14/book.html)

Mathias Paye. Software Security Principles, Policies, and Protection. (January 2019, v0.33) (https://nebelwelt.net/SS3P/softsec.pdf)

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: https://www.microsoft.com/en-us/sdl/
- OWASP SAMM Project: https://www.owasp.org/index.php/OWASP_SAMM_Project
- OWASP TOP 10: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Developer Guide: https://www.owasp.org/index.php/Category:OWASP_Guide_Project
- Testing Guide: https://www.owasp.org/index.php/Category:OWASP_Testing_Project
- Secure Coding Practice Guideline: https://security.berkeley.edu/secure-coding-practice-guidelines
- Seed Labs: https://seedsecuritylabs.org/

Please find more reference materials on the course blackboard website (https://onlinecampus.bu.edu**) (under the Content/References folder)**

Description

Overview of techniques and tools to develop secure software. Focus on application security. Topics include secure software development processes, 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.

Objectives

At the end of the semester, students are expected to

- Explain secure software development process and activities in the process.
- Explain risk management and threat modeling and identify security risks in real world projects.
- Identify common vulnerabilities and corresponding mitigations in C/C++ and Java programs.
- Explain basic cryptographic mechanisms and use right crypto APIs properly.
- Identify common vulnerabilities and corresponding mitigations in web applications and mobile applications.
- Design and conduct security testing for real world applications.

Course Requirements

- Class participation
- Reading and study

- Assignments
    - Labs
    - Written Homeworks
    - Final Project
- Quizzes and Exams

Class Schedule

(This is a tentative class schedule. It is subject to change according to the progress of the class and the feedback of the student.)

Class #	Date	Topics	Assignments
1	01/24	Intro, Secure Software Process, Risk management	Written HW1 (01/24-02/07)
2	01/31	Security Concepts,	Final Project is assigned
3	02/07	Security Principles, MITRE ATT&CK Framework	HW2 (02/07 - 02/21)
4	02/14	Secure Requirements and design, threat modeling	Lab1 (02/14 - 02/28)
5	02/22 (Tue)	Code Review, static code analysis, dynamic code analysis, Vulnerability Taxonomy	Lab 2 (02/21-03/14)
6	02/28	C/C++ Programs Vulnerabilities: memory management, buffer overflow	
7	03/14	C/C++ Programs Vulnerabilities: buffer overflow, integer overflow, string termination problem	Quiz 1 (03/07-03/14) Project Proposal Due
8	03/21	Java Programs Vulnerabilities: visibility issue, reference issue,inner class, reflection, mutability issues, serialization issues	Lab3 (03/28-04/04)

9	03/28	Crypto usage and Misuses vulnerabilities (weak passwords, weak random number, insecure crypto functions etc)	HW3 (03/28 - 04/11)
10	04/04	Crypto Basics, SSL and HTTP, Data Protection	
11	04/11	Browser Security Mechanism, Web Application Security	Lab4 (04/11-04/25)
12	04/20 (Wed)	OWASP Top 10 Mobile Security Mechanisms OWASP Mobile Top 10	Quiz 2 (04/20-05/02)
13	04/25	Risk-based Security Testing/Penetration Testing	
14	05/02	Review/Student Project Presentations	Project is Due
15	05/09	Final Exam	

Course Policies

Grading Policy

The grade that a student receives in this class will be based on class participation, in-class exercises, assignments, quizzes, the final project 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.

- 5% on the class participation
- 40% on written & lab assignments
- 15% on the final project
- 10% on quizzes
- 30% on the final exam

Letter grade/numerical grade conversion is shown below:

A (95-100) A- (90-94)

B+ (85-89) B (80-84) B- (79-77)

C+ (74-76) C (70-73) C- (65-70)

D (60-65) F (0 – 59)

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. The late assignments will be penalized within a week with **3 points per day**. No assignments will be accepted one week after the deadline. It is the students' responsibility to keep secure backups of all assignments.

Academic Integrity

Academic conduct in general and MET College rule in particular require that all references and uses of the work of others must be clearly cited. All instances of plagiarism must be reported to the College for action. *For the full text of the academic conduct code, please check* http://www.bu.edu/met/for-students/met-policies-procedures-resources/academic-conduct-code/.