95-748: Software and Security

Spring 2024

Instructor: Hasan Yasar
hyasar@cmu.edu, 412.268.9219

TA: Sagar Pandita
spandita@andrew.cmu.edu

Fernanda Molina Galindo
fmolinag@andrew.cmu.edu

Location and Time: HBH 1206, Monday, 06:30-09:20PM

Course Description: This course exposes students with limited exposure to programming and software engineering development foundational concepts to enable further understanding of the challenges of insecure and vulnerable software. Students are exposed to basic programming constructs (such as variables, control structures, data structures, programming syntax) as well as the basic principles of object-oriented programming languages. The course also surveys the types of threats and vulnerabilities inherent in software and the origins of these deficiencies. A brief overview of secure coding concepts, principles and techniques are provided to students to provide exposure to how software can be made more secure and resilient and how security can be part of overall software development process.

Textbooks Optional:

- Software Security - Building Security In, Author: Gary McGraw, ISBN: 0321356705
- Agile Application Security: Enabling Security in a Continuous Delivery Pipeline, ISBN: 978-1491938843

Assignments and Grading:

Final course grade:
10% Participation (online discussion/email/chat or participation to the live sessions)
30% Quizzes

60% Project

Participation: Students are expected to participate in class activities and discussions on virtual platform (e.g. live session or discussion board).

Quizzes: Quizzes will be administered through Canvas and will occur weekly. Students will have two days to complete the quiz. There will be a timer set for each quiz lasting between 10 and 15 minutes and students will be forced to complete the quiz once starting the quiz.

Assignment: Assignment assignments will be available via Canvas. Assignment is due on the date specified.

Course Policies:

Late Assignment: Assignment will be accepted up to 3 days late. The maximum grade for the assignment will decrease by 10% for each day late.

Collaboration: Students are encouraged to talk with each other, the TAs, and the instructor about the course and any assignments. Any assistance, though, must be limited to discussion of the problem and sketching general approaches to a solution. Each student must write out his or her own solutions to all problems, unless otherwise stated by the instructor. Consulting another student's or group's solution is prohibited, and submitted solutions may not be copied in any part from any source unless properly cited. These and any other form of unauthorized collaboration on assignments constitute cheating. If you have any questions about whether some activity would constitute cheating, please feel free to ask.

Academic Dishonesty: All instances of cheating or plagiarism will be dealt with according to the "CMU Policy on Cheating and Plagiarism," which can be found at: *http://www.cmu.edu/policies/documents/Cheating.html*. Policy violations will be dealt with on a case-by-case basis. Potential penalties include, but are not limited to, zero credit for the assignment and/or failure of the course.

Course Schedule:

Key Dates: Jan 22nd - First week
Jan 29th - Project Announcement
Feb 29th - Project Due

Course Topics: The following is a brief list of potential course topics:

- Software Security Problems, Principles and Secure Risk Management Framework
- Set of Software Security Best practices
- Secure Software Design and Development
- Software Security in Enterprise Business

Learning Objectives;

- Investigate Software Security Problems and understand Principles and Secure Risk Management Framework
- Understand Set of Software Security Best practices
- Understand and practices Secure Software Design and Development practices
- Learn How to implement Software Security in Enterprise Business

Lectures Plan:

- *January 22nd – Week -1*: Introduction, Software Security Problems

- *January 29th – Week -2*: Software Assurance Model: Risk Management Framework (Ch2), Security Best practices/ Known Security Flaws

- *February 5th – Week -3*: Common Security Vulnerabilities -1 : Security Flaws – Application Low Level Vulnerabilities, Web applications, Cryptographic/Access controls, Networking

- *February 12th – Week-4*: Common Security Vulnerabilities -2 : Security Flaws – Application Low Level Vulnerabilities, Web applications, Cryptographic/Access controls, Networking

- *February 19th – Week -5:* Secure Software Design and Development, Security Testing (Penn testing, Risk- Based Security Testing, Code Review, Architecture Risk Analysis – Ch3, 4,5,6,7)

- *February 26th – Week-6*: Security Testing (Abuse Cases- Operational testing – Ch8,9) Software Security in Enterprise Business/ Large Scale Software Development (Ch10), Review