Course Syllabus Part I
CSD 370 Secure Software Development

3 credit hours

Course Description
This course focuses on providing students with an introduction to the secure software development lifecycle. Topics include current threat landscape, requirements definition, secure design, software implementation, software testing, lifecycle management, deployment, operations, and maintenance. Emphasis is placed on team-based and discovery-based learning methods.

Course Prerequisites
None

Course Objectives
1. Demonstrate an understanding of the basic cybersecurity concepts and the types of adversaries associated with software security.
2. Compare current methodologies used to develop secure software.
3. Explain the processes required in the design phase of secure software development including requirements gathering, attack surface evaluation, and risk assessment.
4. Create a threat model for a given system and analyze results.
5. Describe how to identify vulnerabilities and countermeasures associated with secure software implementation.
6. Demonstrate an understanding of how and when to apply different types of software testing.
7. Identify activities associated with the end stages of secure software lifecycle management.

Grading Scale

Letter Grade	Percentage Grade	Letter Grade	Percentage Grade
A	≥ 92.5%	C	< 76.5% and ≥ 72.5%
A-	< 92.5% and ≥ 89.5%	C-	< 72.5% and ≥ 69.5%
B+	< 89.5% and ≥ 86.5%	D+	< 69.5% and ≥ 66.5%
B	< 86.5% and ≥ 82.5%	D	< 66.5% and ≥ 62.5%
B-	< 82.5% and ≥ 79.5%	D-	< 62.5% and ≥ 59.5%
C+	< 79.5% and ≥ 76.5%	F	< 59.5%

Topic Outline

I. General Security Concepts (Obj. 1)
   A. Security Basics
   B. Security Models
   C. Adversaries
II. Software Development Methodologies (Obj. 2)
   A. Secure Development Lifecycle
   B. Microsoft Security Development
III. Requirements (Obj. 3)
   A. Functional Requirements
   B. Operational Requirements
IV. Secure Software Design (Objs. 3,4)
   a. Processes
   b. Attack Surface Evaluation
   c. Threat Modeling
   d. Risk Assessment for Code Reuse
V. Secure Software Implementation (Obj. 5)
   a. Vulnerabilities and Countermeasures
   b. Defensive Coding Practices
   c. Coding Operations
VI. Secure Software Testing (Obj. 6)
   a. Quality Assurance Testing
   b. Penetration Testing
   c. Simulation Testing
   d. Cryptographic Validation
VII. Secure Software Lifecycle Management (Obj. 7)
   a. Release Activities
   b. Installation and Deployment
   c. Operations and Maintenance

This syllabi update reflects grading scale policy updates effective 4/1/2024.