ITEC 434 (Software Security)

General Information

Course Code	ITEC 434		Required (R)/Selected Elective (SE)			SE
Credit Hours	Theory	2	Lab	1	Total	3
Prerequisites	NIL					
Course Coordinator	Dr. Nithinsha Shajahan					

Course Description

This course explores software security, focusing on identifying and mitigating software application vulnerabilities, threats, and risks. Students will learn to implement security measures and best practices to ensure system reliability and integrity. The curriculum covers designing secure architectures and integrating security into development processes. It emphasizes secure coding practices and evaluates the effectiveness of security measures throughout the software development lifecycle.

Course Objectives

This course aims to provide a comprehensive understanding of software security fundamentals and critical touchpoints, enabling students to analyze various software security issues, including potential vulnerabilities, threats, and risks. It emphasizes implementing effective security assurance measures, applying best practices to ensure software reliability, confidentiality, and integrity. This course focuses on evaluating the secure software development lifecycle, ensuring robust security measures are effectively applied throughout the software development process.

Course Contents

1) Fundamentals of Software Security 2) Software Security Essentials 3) Secure Software Architecture 4) Software Security Assurance 5) Secure Software Development Process 6) Software Security Estimation

Textbook

1. Software Security Concepts & Practices 1st Edition (2023)
2. Gary R. McGraw, Software Security: Building Security

Reference Materials

Allen, Barnum, Ellison, Software Security Engineering: A Guide for Project Managers

Course Learning Outcomes

CLO-1	**Describe** the fundamentals of software security and gain insights into critical software touchpoints to ensure protection against vulnerabilities.
CLO-2	**Identify** various software security issues by assessing potential vulnerabilities, threats, and risks associated with diverse types of software applications.
CLO-3	**Apply** software security assurance measures to maintain the reliability, confidentiality, and integrity of the software systems.
CLO-4	**Design** secure software architectures by developing plans that integrate security principles into the overall structure to mitigate potential threats.
CLO-5	**Evaluate** the secure software development lifecycle by assessing the effectiveness of security measures throughout the software development process.

Course Learning Outcomes

CLO-IDs	Course Learning Objective (CLOs)	Level of Learning (LoL)	Mapped PIs
CLO-1	**Describe** the fundamentals of software security and gain insights into critical software touchpoints to ensure protection against vulnerabilities.	Knowledge	PI 1.2
CLO-2	**Identify** various software security issues by assessing potential vulnerabilities, threats, and risks associated with diverse types of software applications.	Comprehension Applying	PI 1.4 PI 6.4
CLO-3	**Apply** software security assurance measures to maintain the reliability, confidentiality, and integrity of the software systems.	Applying	PI 2.3 PI 6.3
CLO-4	**Design** secure software architectures by developing plans that integrate security principles into the overall structure to mitigate potential threats.	Creating	PI 2.1 PI 6.2
CLO-5	**Evaluate** the secure software development lifecycle by assessing the effectiveness of security measures throughout the software development process.	Evaluating	PI 3.1 PI 3.2

CLO-SO-PI Mapping

	SO-IDs					
CLO IDs	**SO-1**	**SO-2**	**SO-3**	**SO-4**	**SO-5**	**SO-6**
CLO-1	PI 1.2	-	-	-	-	-
CLO-2	PI 1.4	-	-	-	-	PI 6.1
CLO-3	-	PI 2.3	-	-	-	PI 6.4
CLO-4	-	PI 2.1	-	-	-	PI 6.3
CLO-5	-	-	PI 3.1, PI 3.2	-	-	-

Approvals

Prepared by	Dr. Nithinsha Shajahan
Approved by	
Last update	08/01/2025