**Birla Institute of Technology & Science, Pilani**

**Work Integrated Learning Programmes Division**

**\*\*\*\*\*\*\* \*\*\*\*\***

## **Digital Learning** **Handout**

Part A: Content Design

|  |  |
| --- | --- |
| Course Title | Secure Software Engineering |
| Course No(s) | **SE ZG566/SS ZG566** |
| Credit Units | 5 |
| Credit Model | 32-32-64  (32 Hours of Class-room Instruction + 32 Hours of Case-studies/Exploration + 64 Hours of Student Preparation) |
| Instructors | **T V Rao** |
| Version No: |  |
| Date: | 18/01/2025 |

**Course Description**

Best practices for designing secure systems, software engineering principles for designing secure systems, criteria for designing secure systems; analysis of system properties and verification of program correctness; use of formal methods and verification for security; tools for verification of security properties; techniques for software protection and their limitations; analysis of software based attacks (and defences), timing attacks and leakage of information, and type safety.

**Course Objectives**

|  |  |
| --- | --- |
| **No** | **Course Objective** |
| **CO1** | Understand software engineering principles for designing secure systems |
| **CO2** | Learn lifecycle models for software security. |
| **CO3** | Understand software attacks and techniques of building software that can withstand attacks |

**Text Book(s):**

|  |  |
| --- | --- |
| **T1** | Secure, Resilient, and Agile Software Development By Mark Merkow · 2019 |
| **T2** | Computer Security: Principles and Practice by William Stallings, and Lawrie Brown Pearson, 2018. |
| **T3** | Software Security Engineering, Julia H. Allen, et al, Pearson, 2008. |

**Reference Book(s) & other resources:**

|  |  |
| --- | --- |
| **R1** | Application Security Program Handbook. A Guide for Software Engineers and Team Leaders By Derek Fisher · 2022 |
| **R2** | Core Software Security Security at the Source By James Ransome, Anmol Misra · 2018 |
| **R3** | Threat Modelling by Adam Shostack, John Wiley 2014 |

**Learning Outcomes: Students will be able to**

|  |  |
| --- | --- |
| LO1 | Understand causes of security issues in software systems |
| LO2 | Learn practices that enhance security in software development lifecycle. |
| LO3 | Understand techniques of addressing security issues in software |

**Part B: Learning Plan**

|  |  |  |
| --- | --- | --- |
| **Contact Session** | **List of Topic Title** | **Reference** |
| 1 | **M1: Overview of Secure Software Engineering**   * Why Secure Software Engineering ? * Popular Cyber attacks on Software. * Core definitions, concepts, examples. * Differences Product Security versus Security Products | T2, Chapter 1, 6 |
| 2 | **M2:** **Software SDLC**   * Phases in software development * Work products during SDLC * Implications of security requirements on SDLC | T3, Chapter 2,  SWEBOK  Microsoft SDL Documentation |
| 3 | **M3: Product Security Programs**   * Establishing a Security Program * Secure Software Engineering in legacy and agile SDLC models * Shift Right Versus Shift Left * Maturity Models - SAMM , BSIMM * Metrics and Success Criteria | T1, Chapter 3, 11 ; R1, Chapter 1 |
| 4 | **M4: Threat modelling**   * Principles of threat modelling * OWASP (Open Web Application Security Project) threat modelling process * Microsoft approach to threat modelling | R3, Ch 2  Threat Modeling Process of OWASP Foundation |
| 5 | **M5: Product Security Requirements**   * Software Requirements - Functional and Nonfunctional * Product Security Baselines * Microsoft and OWASP recommendations | T3 Chapter 3 ;  Microsoft SDL Documentation |
| 6 | **M6: Secure Design & Architecture**   * Risk Assessments * Principles for secure design * Security Constructs - Authentication, Authorization, Encryption, Logging * Secure patterns | T3 Chapter 4 ,  R2 Chapter 4 |
| 7 | **M7:** **Security Testing**   * Unit Testing for Security * Static Application Security Testing (SAST) * Dynamic Application Security Testing (DAST) * Interactive Application Security Testing (IAST) * Fuzz Testing & Brute Forcing * Penetration Testing | T1 Chapter 8, 9  T3 Chapter 5 |
| 8 | **M8: Secure Coding**   * Popular security vulnerabilities * Defensive Programming and Secure Coding Practices (by examples) * Secure Code Review | T1, Chapter 7 |
| 9 | **M8: Secure Coding (Buffer Overflows)**   * Buffer overflow and defences * Heap, integer, and format string vulnerabilities * Java security | T2, Chapter 10, 11 |
| 10 | **M8: Secure Coding (Database Security)**   * Discretionary & mandatory access control. Bell LaPadula model * Statistical and flow controls * SQL injection | T2, Chapter 5 |
| 11 | **M8: Secure Coding (Web Application Security)**   * Vulnerabilities in web development tools * Vulnerabilities in web environment * XSS and Variants | T2, Chapter 11 |
| 12 | **M9: Software Transparency**   * Supply Chain Security * Software Composition Analysis (SCA) * Software Bill of Materials (SBOM) * Open Source Security (OpenSSF) * Building Trustworthy Systems - Hardware and Software | R1, Chapter 4  R2, Chapter 8 |
| 13 | **M10: Secure Deployment and Operations**   * System Hardening * Runtime Application Security Protection (RASP) * Securing Data Centers, Hardware Manufacturing factories * Security Monitoring – Applications * IDS/IPS | T1, Chapter 9,  T2, Chapter 8, 9 |
| 14 | **M11:** **Security Mechanisms**   * Encryption * Source Code Signing, Image Signing * AI in Security | T2, Chapter 20, 21 |
| 15 | **M12: Post Deployment and Response**   * Vulnerability Response, Security Advisories - Standards and Best Practices * Incident Response * Responsible Disclosure and Stakeholder Management * Governance for Security * Risk Management | T2, Chapter 14, 15  R2, Chapter 8 |
| 16 | **Review** | Entire Syllabus |

**Experiential Learning Components:**

1. Quiz 1
2. Quiz 2
3. Assignment

**Objective of Experiential Learning Component:** Application of concepts explained in lectures

**Scope of Experiential Learning Component:** Understanding real-life scenarios and appropriately managing security

**Lab Infrastructure:** Not Applicable

**List of Experiments:** Not Applicable

**Evaluation Scheme:**

**Legend:** EC = Evaluation Component; AN = After Noon Session; FN = Fore Noon Session

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| EC | Name | Type | Weight | Duration | Date, Session, Time |
| EC – 1 | Quiz 1 | Online | 5% | 8 days | Mar 2nd – Mar 9th |
|  | Quiz 2 | Online | 5 % | 8 days | Apr 24th – May 1st |
|  | Assignment | Online | 20 % | 15 days | May 1st - May 16th |
| EC - 2 | Mid-Semester Test | Closed Book | 25% | 2 hours | •Regular – Mar 21-23  •Make-up – Apr 4-6 |
| EC - 3 | Comprehensive Exam | Open Book | 45% | 2 ½ Hours | •Regular – May 23-25  •Make-up – May 30-31, Jun 1 |

EC1: = 30%

Syllabus for Mid-Semester Test (Closed Book): Topics in Contact session: 1 to 8

Syllabus for Comprehensive Exam (Open Book): All topics

**Important Links and Information:**

**eLearn Portal:** [https://elearn.bits-pilani.ac.in](https://elearn.bits-pilani.ac.in/)

Students must visit the eLearn portal regularly and stay updated with the latest announcements and deadlines.

**Contact Sessions:** Students should attend the online lectures as per the schedule provided on the eLearn portal.

**Evaluation Guidelines:**

1. EC-1 consists of two Quizzes and an Assignment. Students will attempt them through the course pages on the eLearn portal. Announcements will be made on the portal in a timely manner.
2. For Closed Book tests: No books or reference material of any kind will be permitted.
3. For Open Book exams: “open book” means text/ reference books (publisher copy only) and does not include any other learning material. No other learning material will be permitted during the open book examinations. For Detailed Guidelines refer to the attached document.

[EC3 Guidelines](https://docs.google.com/document/d/1DJvlhVzOaIw4njc9g30MlBuu0DqTzeIL/edit?usp=drive_link&ouid=104481483083011111295&rtpof=true&sd=true)

1. If a student is unable to appear for the Regular Test/Exam due to genuine exigencies, the student should follow the procedure to apply for the Make-Up Test/Exam, which will be made available on the eLearn portal. The Make-Up Test/Exam will be conducted only at selected exam centres on the dates to be announced later.

It shall be the responsibility of the individual student to be regular in maintaining the self-study schedule as given in the course handout, attend the online lectures, and take all the prescribed evaluation components such as Assignments/Quizzes, Mid-Semester Tests and Comprehensive Exams according to the evaluation scheme provided in the handout.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*