

**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI**

**WORK INTEGRATED LEARNING PROGRAMMES**

**COURSE HANDOUT**

**Part A: Content Design**

|  |  |
| --- | --- |
| **Course Title** | Secure Software Engineering |
| **Course No(s)** | SE ZG566/SS ZG566 |
| **Credit Units** | 5 |
| **Course Author** | Madhu B K |
| **Version No** |  |
| **Date** |  |

**Course Description**

|  |
| --- |
| Secure software engineering focuses on creating software that functions correctly even when attacked. The main topics of this course include requirements engineering for secure software, secure software architecture and design, considerations for secure coding and testing, common software vulnerabilities, risk analysis, misuse cases, secure programming techniques, analysis of software-based attacks (and defences), code reviews, and security testing. |

**Course Objectives**

|  |  |
| --- | --- |
| **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 |

**Textbooks**

|  |  |
| --- | --- |
| T1 | Software Security Engineering, Julia H. Allen, et al, Pearson, 2008. |
| T2 | Computer Security: Principles and Practice by William Stallings, and Lawrie Brown Pearson, 2018. |

**Reference Books**

|  |  |
| --- | --- |
| R1 | Security in Computing by Charles P. Pfleeger, Shari L. Pfleeger, and Deven Shah Pearson Education 2009 |
| R2 | Threat Modelling by Adam Shostack, John Wiley 2014 |
| R3 | Public sources viz. OWASP, www.cert.org, www.buildsecurityin.com etc. |

**Modular Structure**

|  |  |
| --- | --- |
| **No** | **Title of the Module** |
| M1 | Overview of security |
| M2 | Security in SDLC |
| M3 | Threat Modelling |
| M4 | Security Requirements Engineering |
| M5 | Secure Architecture & Design |
| M6 | Testing for security |
| M7 | Vulnerabilities in code |
| M8 | Database security |
| M9 | Web Application Security |
| M10 | Security Mechanisms |
| M11 | Managing for security |

**Learning Outcomes:**

|  |  |
| --- | --- |
| **No** | **Learning Outcomes** |
| **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: Contact Session Plan**

|  |  |
| --- | --- |
| **Academic Term** | First Semester 2023-2024 |
| **Course Title** | Secure Software Engineering |
| **Course No** | SE ZG566/SS ZG566 |
| **Lead Instructor** | Madhu BK |

## Glossary of Terms

1. Contact Hour (CH) stands for a hour long live session with students conducted either in a physical classroom or enabled through technology. In this model of instruction, instructor led sessions will be for 22 CH.
   1. Pre CH = Self Learning done prior to a given contact hour
   2. During CH = Content to be discussed during the contact hour by the course instructor
   3. Post CH = Self Learning done post the contact hour
2. Contact Hour (CS) stands for a two-hour long live session with students conducted either in a physical classroom or enabled through technology. In this model of instruction, instructor led sessions will be for 11 CS.
   1. Pre CS = Self Learning done prior to a given contact session
   2. During CS = Content to be discussed during the contact session by the course instructor
   3. Post CS = Self Learning done post the contact session
3. RL stands for Recorded Lecture or Recorded Lesson. It is presented to the student through an online portal. A given RL unfolds as a sequences of video segments interleaved with exercises
4. SS stands for Self-Study to be done as a study of relevant sections from textbooks and reference books. It could also include study of external resources.
5. LE stands for Lab Exercises
6. HW stands for Home Work.
7. M stands for module. Module is a standalone quantum of designed content. A typical course is delivered using a string of modules. M2 means module 2.

## Teaching Methodology (Flipped Learning Model)

The pedagogy for this course is centered around flipped learning model in which the traditional class-room instruction is replaced with recorded lectures to be watched at home as per the student’s convenience and the erstwhile home-working or tutorials become the focus of classroom contact sessions. Students are expected to finish the home works on time.

## Contact Session Plan

* Each Module (M#) covers an independent topic and module may encompass more than one Recorded Lecture (RL).
* Contact Sessions **(2hrs each week)** are scheduled alternate weeks after the student watches all Recorded Lectures (RLs) of the specified Modules (listed below) during the previous week
* In the flipped learning model, Contact Sessions are meant for in-classroom discussions on cases, tutorials/exercises or responding to student’s questions/clarification--- may encompass more than one Module/RLs/CS topic.
* Contact Session topics listed in course structure (numbered CSx.y) may cover several RLs; and as per the pace of instructor/students’ learning, the instructor may take up more than one CS topic during each of the below sessions.

## Detailed Structure

**Introductory Video/Document:** *<< Introducing the faculty, overview of the course, structure and organization of topics, guidance for navigating the content, and expectations from students>>*

* Each of the sub-modules of **Recorded Lectures** (RLx.y ) shall delivered via **30 – 60mins videos** followed by:
* **Contact session** (CSx.y) of 2Hr each for illustrating the concepts discussed in the videos with exercises, tutorials and discussion on case-problems (wherever appropriate); contact sessions (CS) may cover more than one recorded-lecture (RL) videos.

## Course Contents

**M1: Overview of security**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL1.1 | The definitions and concepts of security |  |
| RL1.2 | Threats to software/assets |  |
| RL1.3 | Malware Nomenclature |  |
| During CS | CS1.1 | Review security basics (T1, Ch 1) |  |
| CS1.2 | Discuss software security environment (T1, Ch 1) |  |
| Post-CS | SS1.1 | Self-Study (T1, Chapter 1; T2, Chapter 1) |  |
| HW1.1 | Do exercises given at the end of chapter 1 of T1 |  |

**M2: Security in SDLC**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL2.1 | Phases in software development |  |
| RL2.2 | Work products during SDLC |  |
| RL2.3 | Implications of security requirements on SDLC |  |
| During CS | CS2.1 | Review SDLC and Work Products |  |
| CS2.2 | Discuss modifications to work products due to Security |  |
| Post-CS | SS2.1 | Self-Study (T1, Chapter 2) |  |
| HW2.1 | Do exercises given at the end of chapter 2 of T1 |  |

**M3: Threat Modelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL3.1 | Principles of threat modelling |  |
| RL3.2 | OWASP (Open Web Application Security Project) threat modelling process |  |
| RL3.3 | Microsoft approach to threat modelling |  |
| During CS | CS3.1 | Review threat modelling basics |  |
| CS3.2 | Discuss threats to various software |  |
| Post-CS | SS3.1 | Self-Study (R3, Chapter 2) |  |
| HW3.1 | Identify threats for an application |  |

**M4: Security Requirements Engineering**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL4.1 | Incorporating security during requirements gathering |  |
| RL4.2 | CMU SQUARE process model |  |
| RL4.3 | Microsoft and OWASP recommendations |  |
| During CS | CS4.1 | Review Security Requirements Engineering |  |
| CS4.2 | Discuss security requirements work products |  |
| Post-CS | SS4.1 | Self-Study (T1, Chapter 3) |  |
| HW4.1 | Build work products for an application |  |

**M5: Secure Architecture & Design**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL5.1 | Security incorporation in architecture & design process |  |
| RL5.2 | Principles for secure design |  |
| RL5.3 | Secure patterns |  |
| During CS | CS5.1 | Review design and architecture for security |  |
| CS5.2 | Discuss security work products for architecture & design |  |
| Post-CS | SS5.1 | Self-Study (T1, Chapter 4) |  |
| HW5.1 | Build work products for an application |  |

**M6: Testing for security**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL6.1 | Secure testing concepts |  |
| RL6.2 | Source code analysers |  |
| RL6.3 | White box testing for security |  |
| RL6.4 | Black box testing for security |  |
| During CS | CS6.1 | Review testing for security |  |
| CS6.2 | Discuss testing tools |  |
| CS6.3 | Discuss test methods/cases |  |
| Post-CS | SS6.1 | Self-Study (T1, Chapter 5) |  |
| HW6.1 | Build test cases for familiar applications |  |

**M7: Vulnerabilities in code**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL7.1 | Buffer overflow and defences |  |
| RL7.2 | Heap, integer, and format string vulnerabilities |  |
| RL7.3 | Java security |  |
| During CS | CS7.1 | Review vulnerabilities in code |  |
| CS7.2 | Examples of code vulnerabilities |  |
| Post-CS | SS7.1 | Self-Study (T2, Chapter 10, 11) |  |
| HW7.1 | Do exercises given at the end of chapter 11, 12 of T2 |  |

**M8: Database security**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL8.1 | Discretionary & mandatory access control. Bell LaPadula model |  |
| RL8.2 | Statistical and flow controls |  |
| RL8.3 | SQL injection |  |
| During CS | CS8.1 | Review database security |  |
| CS8.2 | Examples of vulnerabilities in database/SQL |  |
| Post-CS | SS8.1 | Self-Study (T2, Chapter 5) |  |
| HW8.1 | Do exercises given at the end of chapter 5 of T2 |  |

**M9: Web Application Security**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL9.1 | Vulnerabilities in web development tools |  |
| RL9.2 | XSS |  |
| During CS | CS9.1 | Review web application security |  |
| CS9.2 | Examples of vulnerabilities in web applications |  |
| Post-CS | SS9.1 | Self-Study (T2, Chapters 11) |  |
| HW9.1 | Do exercises given at the end of chapter 21 of T2 |  |

**M10: Security Mechanisms**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL10.1 | Encryption for security |  |
| RL10.2 | Digital signatures |  |
| RL10.3 | Intrusion detection |  |
| RL10.4 | Intrusion prevention |  |
| During CS | CS10.1 | Review security mechanisms |  |
| CS10.2 | Discuss examples of various security mechanisms |  |
| Post-CS | SS10.1 | Self-study (T2, Chapter 8, 9) |  |
| HW10.1 | Do exercises given at the end of chapter 2, 6 of T2 |  |

**M11: Managing for security**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CS | RL11.1 | Governance for security |  |
| RL11.2 | Risk management |  |
| RL11.2 | Security incident handling |  |
| During CS | CS11.1 | Review management for security |  |
| CS11.2 | Discuss examples risk management and incident handling |  |
| Post-CS | SS11.1 | Self-Study (T1, Chapter 7) |  |
| HW11.1 | Prepare management work products. |  |

**Experiential Learning Components:**

|  |  |  |
| --- | --- | --- |
| **Topics No.** | **Select Topics in Syllabus for experiential learning** | **Access URL** |
| 1 | Requirements Analysis for Security |  |
| 2 | Architecture and Design for Security |  |
| 3 | Vulnerabilities/Defences in Coding |  |

**Evaluation Scheme**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No** | **Name** | **Type** | **Duration** | **Weight** | **Day, Date, Session, Time** |
| EC-1 | Quiz-1 | | \* | 10% | September 1-10, 2023 |
| Quiz-2 | | \* | 10% | October 1-10, 2023 |
| Assignment | | \* | 10% | November 1-10, 2023 |
| EC-2 | Mid-Semester Test | Close Book | 2 hours | 30% | Saturday, 23/09/2023 (Evening) |
| EC-3 | Comprehensive Exam | Open Book | 2 ½ hours | 40% | Saturday, 25/11/2023 (Evening) |

***Note*** *- Evaluation components can be tailored depending on the proposed model.*

**Important Information**

Syllabus for Mid-Semester Test (Close Book): Topics in Weeks 1-7

Syllabus for Comprehensive Exam (Open Book): All topics given in plan of study

Evaluation Guidelines:

1. EC-1 consists of either two Assignments or three Quizzes. Announcements regarding the same will be made in a timely manner.
2. For Closed Book tests: No books or reference material of any kind will be permitted. Laptops/Mobiles of any kind are not allowed. Exchange of any material is not allowed.
3. For Open Book exams: Use of prescribed and reference text books, in original (not photocopies) is permitted. Class notes/slides as reference material in filed or bound form is permitted. However, loose sheets of paper will not be allowed. Use of calculators is permitted in all exams. Laptops/Mobiles of any kind are not allowed. Exchange of any material is not allowed.
4. 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. The genuineness of the reason for absence in the Regular Exam shall be assessed prior to giving permission to appear for the Make-up Exam. 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 lectures, and take all the prescribed evaluation components such as Assignment/Quiz, Mid-Semester Test and Comprehensive Exam according to the evaluation scheme provided in the handout.