INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

SECURITY THREATS AND MODELLING

V Semester: CSE

Course Code	Category	Hours / Week			Credits	Maximum Marks		
ACSD23	Core	L	T	P	C	CIA	SEE	Total
		3	0	0	3	40	60	100
Contact Classes: 48	Tutorial Classes: Nil	Practical Classes: Nil				Total Classes: 48		
Prerequisites: Computer Networks								

I. COURSE OVERVIEW:

This course provides a comprehensive understanding of the principles, techniques, and tools used to identify, assess, and mitigate security threats in software and system architectures. Students will explore various threat modelling methodologies such as STRIDE, DREAD, Microsoft SDL, PASTA, OCTAVE, and Trike. The course emphasizes the use of visual tools like data flow diagrams (DFDs) and attack trees to analyze system vulnerabilities.

II. COURSES OBJECTIVES:

The students will try to learn:

I The fundamentals of information security, including types of threats, vulnerabilities, and common attack strategies on systems and networks.

II The threat modelling techniques to identify, assess, and mitigate security threats in software, systems, and network architectures.

III Apply visual modeling techniques like Attack Trees and DFDs to analyze security boundaries and integrate threat analysis into secure system design.

III. COURSE OUTCOMES:

At the end of the course, students should be able to:

CO1	Identify various types of security threats, vulnerabilities, and attack vectors.
CO2	Apply threat modelling techniques such as STRIDE and DREAD to analyze system risks.
CO3	Evaluate different threat modelling methodologies like SDL, PASTA, OCTAVE, and Trike.
CO4	Design secure systems using attack trees, DFDs, and threat mitigation strategies.
CO5	Use threat modelling tools to simulate and manage threats in real-world applications.
CO6	Identify various types of security threats, vulnerabilities, and attack vectors.

IV. COURSE CONTENT:

MODULE –I: INTRODUCTION TO SECURITY THREATS (10)

Introduction: Basic Terminologies: Threat, Vulnerability, Risk, Attack, Types of Threats: Insider, Outsider, Physical, Network-based, Malware: Viruses, Worms, Trojans, Ransomware, Cyber Attacks: Phishing, Spoofing, SQL Injection, DoS/DDoS, Security Goals: Confidentiality, Integrity, Availability (CIA).

MODULE –II: FUNDAMENTALS OF THREAT MODELLING (10)

Need for Threat Modelling, Threat Modelling Lifecycle, Key Elements: Assets, Attackers, Entry Points, Trust Boundaries, STRIDE Threat Classification Model, Threat Modelling in SDLC (Software Development Lifecycle)

MODULE –III: THREAT MODELLING METHODOLOGIES (09)

Overview of Methodologies: Microsoft SDL, Secure-by-design principles, Threat modelling integrated into SDLC, PASTA(Process for Attack Simulation and Threat Analysis), 7-stage methodology (Defining Objectives to Residual Risk Analysis), Focuses on attacker perspective and business impact, OCTAVE, Trike, Use of Attack Trees and Data Flow Diagrams (DFDs).

Risk Rating: Introduction to DREAD Model, Prioritizing Threats Based on Risk, CVSS (Common Vulnerability Scoring System), Qualitative vs Quantitative Risk Analysis, Risk Matrix (Likelihood Impact).

MODULE –IV: RISK MANAGEMENT AND MITIGATION (09)

Risk Assessment: Identifying & Evaluating Risks, Mitigation Strategies and Countermeasures, Secure Design Principles, Security Testing and Validation, Security Documentation and Threat Modelling Reports.

MODULE –V: TOOLS AND APPLICATIONS (10)

Microsoft Threat Modelling Tool, OWASP Threat Dragon, Introduction to CAIRIS and Threat Spec, Real-time Case Studies: Web App, IoT Device, Cloud System, Industry Use-Cases: E-Governance, FinTech, Healthcare

V. TEXTBOOKS:

1. Adam Shostack, “*Threat Modelling: Designing for Security”*, Wiley. 1st Edition, 2013
2. Michael Howard & Steve Lipner, “*The Security Development Lifecycle”*, Microsoft Press, 1st Edition, 2013.
3. Whitman & Mattord, “*Principles of Information Security”*, Cengage Learning, 1st Edition, 2009.

VI. REFERENCE BOOKS:

1. NIST SP 800-154, Guide to Data-Centric System Threat Modelling, 1st Edition, 2009
2. William Stallings and Lawrie Brown, “Computer Security: Principles and Practice”, 1st Edition, 2009.
3. Software Security: Building Security In” – Gary McGraw, 1st Edition, 2011.

VII. ELECTRONICS RESOURCES:

1. https://www.udemy.com/course/google-cyber-security-leader-certification/?couponCode=ST8MT40924
2. www.udemy.com/courses/search/?q=microsoft+threat-modeling&src=sac&kw=microsoft+Ahttps://www.edx.org/l

VIII. MATERIALS ONLINE:

1. Course Outline Description
2. Tutorial question bank
3. Tech talk topics

4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. PowerPoint presentation
11. E-Learning Readiness Videos (ELRV)