Mehran University of Engineering and Technology, Jamshoro
Department of Software Engineering

Title of Subject	**:**	**Software Security (SE605)**
Discipline	**:**	Software Engineering (1st Semester)
Effective	**:**	24MESE & onwards
Pre-requisite	**:**	--
Assessment	**:**	Theory**:** 10% Sessional, 30% Mid, 60% Final
Credit Hours	**:**	3 + 0 **Marks:** 100
Minimum Contact Hours:		42

Objectives of course:

- To elucidate fundamental principles of software security, encompassing design principles, cryptography, risk management, and ethical considerations.
- To analyze the legal, ethical, and professional aspects relevant to software security.
- To utilize diverse security and risk management tools to establish and maintain software security and privacy.
- To employ suitable methodologies to address and resolve challenges within the field of software security.

Course outline:

- Advanced Information Security Concepts
- Threat Modeling for Complex Systems
- Security in Distributed and Cloud Environments
- Resilient and Adaptive Security Architectures
- Secure Software Design and Development
- Secure Application Architectures (e.g., Microservices, Serverless)
- Security Patterns and Anti-Patterns
- Threat Modeling and Risk Assessment in Depth
- Advanced Cryptography for Software Security
- Post-Quantum Cryptography
- Homomorphic Encryption and Multi-Party Computation
- Formally Verified Cryptographic Protocols
- Key Management and Secure Protocols
- Hardware Security Modules (HSMs) and Trusted Execution Environments (TEEs)
- Key Splitting and Secret Sharing Schemes
- Side-Channel Attacks and Countermeasures
- Advanced Software Threats and Protections
- Advanced Web Application Security
- Advanced Mobile Application Security
- Advanced Malware Analysis and Defense
- Database Security and Privacy
- Database Intrusion Detection and Prevention
- Privacy-Preserving Data Analysis
- Secure Aggregation and Data Anonymization
- Advanced Network Security
- Next-Generation Firewalls and Application-Layer Filtering
- Behavioral-Based Network Security
- Threat Hunting and Cyber Threat Intelligence
- Security Policies, Compliance, and Risk Management
- Security Policy Frameworks and Standards
- Policy-Based Security Automation
- Quantitative Risk Assessment Techniques

- Emerging Trends in Software Security
- IoT Security and Embedded Systems Security
- Blockchain Security
- Decentralized Identity and Privacy on the Blockchain

BOOKS RECOMMENDED

1. William Stallings and Awrie Brown Computer Security: Principles and Practice, Paerson, Latest edition

2. M. Whitman and H. Mattord, Principles of Information Security, Cengage Learning, Latest Edition.

3. Dieter Gollmann, Computer Security, Wiley, Latest Edition.

4. William Easttom, Computer Security Fundamentals, Pearson IT Certification, Latest Edition.

5. Steven Hernandez CISSP, Official (ISC)2 Guide to the CISSP CBK, Auerbach Publications, Latest Edition

Approval:

Board of Studies:	**Resolution No. 2.3**	**Dated: 21-07-2023**
Board of Faculty:	**Resolution No. 21.9**	**Dated: 07-12-2023**
AR&RB	**Resolution No.**	
Academic Council:	**Resolution No.**	