National University of Engineering (UNI)
School of Artificial Intelligence
Syllabus 2027-I

1. COURSE

CS3I1. Computer Security (Mandatory)

2. GENERAL INFORMATION

2.1 Course	:	CS3I1. Computer Security
2.2 Semester	:	9th Semester.
2.3 Credits	:	3
2.4 Hours	:	1 HT; 4 HP;
2.5 Duration of the period	:	16 weeks
2.6 Type of course	:	Mandatory
2.7 Learning modality	:	Face to face
2.8 Prerrequisites	:	CS231. Networking and Communication. (7th Sem)

3. PROFESSORS

Meetings after coordination with the professor

4. INTRODUCTION TO THE COURSE

In an increasingly digital world, security is no longer an optional feature but a fundamental requirement. This course provides a comprehensive introduction to the principles and practices of cybersecurity, covering everything from theoretical foundations to secure coding and digital forensics. Students will gain the skills necessary to design, implement, and govern secure systems while understanding the ethical and professional responsibilities involved in protecting information and infrastructure.

5. GOALS

- Understand the fundamental principles and mathematical bases of security.
- Apply secure coding techniques and cryptographic methods to software.
- Analyze system vulnerabilities and perform forensic investigations.
- Evaluate security governance and professional ethics in cybersecurity.

6. COMPETENCES

AG-C09) Design and Development of Solutions: Designs, implements, and evaluates solutions for complex computing problems. (Usage)

AG-C11) Use of Tools: Applies modern computing tools in problem solving. (Usage)

7. TOPICS

Unit 1: Security Mindset and Principles (6 hours)	
Competences Expected: AG-C09,AG-C11	
Topics	**Learning Outcomes**
• Developing a security mindset incorporating cross-cutting concepts: confidentiality, integrity, availability, risk assessment, systems thinking, adversarial thinking, human-centered thinking. • Vulnerabilities, threats, attack surfaces, and attack vectors Protection and Safety. • Denial of Service (DoS) and Distributed Denial of Service (DDoS) Protection and Safety. • Principles and practices of protection, e.g., least privilege, open design, fail-safe defaults, defense in depth, and zero trust; and how they can be implemented Principles of Operating System, Protection and Safety, Coding Practices, Large-Scale Construction and Process, Computer Crimes and Attacks, Security Laws, Policies and Responsibility. • Optimization considerations between security, privacy, performance, and other design goals System Design, Software Development Practices, Performance Testing and Benchmarking, Testing Tools and Analysis, Verification and validation Concepts, Test Planning and Types, Advanced Testing Practices. • Concepts of trust and trustworthiness.	• Evaluate a system for possible attacks that can be launched by an adversary [Evaluate] • Design and develop approaches to protect a system from a set of identified threats [Design] • Describe how harm to user privacy can be avoided [Describe] • Develop a system that incorporates various principles of security and privacy [Create]
Readings : [**Pfleeger2015**], [**Stallings2017**]	

Unit 2: Cryptography Fundamentals (8 hours)	
Competences Expected: AG-C09,AG-C11	
Topics	**Learning Outcomes**
• Differences between algorithmic, applied, and mathematical views of cryptography. • Mathematical preliminaries: modular arithmetic, Euclidean algorithm, probabilistic independence, linear algebra basics, number theory, finite fields, complexity, asymptotic analysis Discrete Mathematics, Linear Algebra. • Basic cryptography: symmetric key and public key cryptography Foundational Data Structures, Foundational Algorithms, Advanced Algorithms, Discrete Mathematics. • Classical cryptosystems, such as shift, substitution, transposition ciphers, code books, and machines Discrete Mathematics. • Kerckhoff's principle and use of vetted libraries Coding Practices, Large-Scale Construction and Process.	• Explain the role of cryptography in supporting security and privacy [Explain] • Discuss the risks of inventing one's own cryptographic methods [Debate] • Discuss the importance of prime numbers in cryptography and explain their use in cryptographic algorithms [Debate] • Implement and cryptanalyze classical ciphers [Implement]
Readings : [**Stallings2017**]	

Unit 3: Injection and Input Validation (8 hours)	
Competences Expected: AG-C09,AG-C11	
Topics	**Learning Outcomes**
• Common vulnerabilities and weaknesses. • SQL injection and other injection attacks. • Cross-site scripting techniques and mitigations. • Input validation and data sanitization Protection and Safety, Basic Programming Concepts and Constructs, Programming Practices: Testing, Debugging, and Documentation, Performance Testing and Benchmarking, Testing Tools and Analysis, Verification and validation Concepts, Test Planning and Types, Advanced Testing Practices.	• Identify underlying problems in given examples of an enumeration of common weaknesses and explain how they can be circumvented [Analyze] • Apply input validation and data sanitization techniques to enhance security of a program [Apply] • Evaluate and prevent SQL injections attacks on a database application [Evaluate] • Evaluate and prevent cross-site scripting attacks against a website [Evaluate] • Construct a program that tests for all input handling errors [Create]
Readings : [**Pfleeger2015**]	

Unit 4: Malware Analysis and Advanced Security (6 hours)	
Competences Expected: AG-C09	
Topics	**Learning Outcomes**
• Offensive security techniques as a defense. • AI-assisted malware detection techniques. • Ransomware: creation, prevention, and mitigation. • Secure use of third-party components Coding Practices, Large-Scale Construction and Process, Performance Testing and Benchmarking, Testing Tools and Analysis, Verification and validation Concepts, Test Planning and Types, Advanced Testing Practices. • Malware: varieties, creation, reverse engineering, and defense against them Language Translation and Execution, Systems Execution and Memory Model. • Assurance: testing (including fuzzing and penetration testing), verification, and validation Protection and Safety, Basic Programming Concepts and Constructs, Programming Practices: Testing, Debugging, and Documentation, Coding Practices, Large-Scale Construction and Process, Performance Testing and Benchmarking, Testing Tools and Analysis, Verification and validation Concepts, Test Planning and Types, Advanced Testing Practices. • Static and dynamic analyses Program Analysis and Analyzers, Protection and Safety, Evaluation, Performance Testing and Benchmarking, Testing Tools and Analysis, Verification and validation Concepts, Test Planning and Types, Advanced Testing Practices. • Secure compilers and secure code generation Language Translation and Execution, Run-time Behavior and Systems.	• Describe different kinds of malicious software [Describe] • Explain the risks of misusing interfaces with third-party code and how to correctly use third-party code [Explain] • Discuss the need to update software to fix security vulnerabilities and the lifecycle management of the fix [Debate] • Apply static and dynamic tools to identify programming faults [Apply] • Evaluate a system for the existence of malware and remove it [Evaluate] • Implement preventive techniques to reduce the occurrence of ransomware [Implement]
Readings : [**SikorskiHonig2012**], [**Eilam2005**], [**NIST800-53**]	

Unit 5: Threat Analysis and Security Engineering (8 hours)	
Competences Expected: AG-C09,AG-C11	
Topics	**Learning Outcomes**
• Security engineering goals: building systems that remain dependable despite errors, accidents, or malicious adversaries Coding Practices, Large-Scale Construction and Process, Performance Testing and Benchmarking, Testing Tools and Analysis, Verification and validation Concepts, Test Planning and Types, Advanced Testing Practices, Computer Crimes and Attacks, Security Laws, Policies and Responsibility. • Problem analysis and situational analysis to address system security Performance Testing and Benchmarking, Testing Tools and Analysis, Verification and validation Concepts, Test Planning and Types, Advanced Testing Practices. • Security analysis, covering security requirements analysis; security controls analysis; threat analysis; and vulnerability analysis Program Analysis and Analyzers, Evaluation. • Security attack domains and attack surfaces, e.g., communications and networking, hardware, physical, social engineering, software, and supply chain Network Security. • Security attack modes, techniques, and tactics, e.g., authentication abuse; brute force; buffer manipulation; code injection; content insertion; denial of service; eavesdropping; function bypass; impersonation; integrity attack; interception; phishing; protocol analysis; privilege abuse; spoofing; and traffic injection Network Security, Protection and Safety, Performance Testing and Benchmarking, Testing Tools and Analysis, Verification and validation Concepts, Test Planning and Types, Advanced Testing Practices.	• Create a threat model for a system or system design [Create] • Apply situational analysis to develop secure solutions under a specified scenario [Apply] • Identify and mitigate security vulnerabilities and weaknesses in a system [Analyze]
Readings : [**Anderson2020**]	

Unit 6: Digital Forensics Techniques (6 hours)	
Competences Expected: AG-C09,AG-C11	
Topics	**Learning Outcomes**
• Basic principles and methodologies for digital forensics. • System design for forensics. • Forensics in different situations: operating systems, file systems, application forensics, web forensics, network forensics, mobile device forensics, use of database auditing Network Security. • Attacks on forensics and preventing such attacks.	• Explain what a digital investigation is and how it can be implemented Computer Crimes and Attacks, Security Laws, Policies and Responsibility [Explain] • Design and implement software to support forensics [Design] • Extract data from a hard drive to comply with the law Computer Crimes and Attacks, Security Laws, Policies and Responsibility [Extract] • Recover data based on a given search term from an imaged system [Analyze] • Reconstruct data and events from an application history, or a web artifact, or a cloud database, or a mobile device. Mobile Platforms: Capabilities and Asynchronous Computing, Mobile Platforms: Architecture and Constraints, Mobile Platforms: Development Fundamentals, Cloud Architecture and Data Management, Frontend, Frameworks and Web Standards [Apply] • Capture and analyze network traffic. Network Security [Analyze] • Develop approaches to address the challenges associated with mobile device forensics [Create] • Apply forensics tools to investigate security breaches [Apply] • Identify and mitigate anti-forensic methods [Analyze]
Readings : [**Pfleeger2015**]	

Unit 7: Security Governance, Management and Policy (6 hours)	
Competences Expected: AG-C09,AG-C11	
Topics	**Learning Outcomes**
• Protecting critical assets from threats. • Security governance: organizational objectives and general risk assessment. • Security management: achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability Performance Testing and Benchmarking, Testing Tools and Analysis, Verification and validation Concepts, Test Planning and Types, Advanced Testing Practices. • Security policy: organizational policies, issue-specific policies, system-specific policies.	• Describe critical assets and how they can be protected [Describe] • Differentiate between security governance, management, and controls, giving examples of each [Differentiate] • Describe a technical control and implement it to mitigate specific threats [Describe]
Readings : [**Anderson2020**]	

Unit 8: Security Ethics, Law and Society (6 hours)	
Competences Expected: AG-C09,AG-C11	
Topics	**Learning Outcomes**
• Societal impacts on breakdowns in security and privacy Digital Equity and Accessibility, Social Impact and AI, Civil Liberties and Expression, Data, Surveillance and Privacy Technology, Privacy Philosophical Foundations and Legislation, Computer Crimes and Attacks, Security Laws, Policies and Responsibility. • Applicability of laws and regulations on security and privacy Computer Crimes and Attacks, Security Laws, Policies and Responsibility. • Professional ethical considerations when designing secure systems and maintaining privacy; ethical hacking Civil Liberties and Expression, Data, Surveillance and Privacy Technology, Privacy Philosophical Foundations and Legislation, Ethics Codes and Legal Accountability, Professional Responsibility and Public Policy, Professional Values, Nature and Continuing Development, Ethical Dissent and Cultural Context, Workplace Ethics, Computer Crimes and Attacks, Security Laws, Policies and Responsibility. • Security and privacy implications of malicious AI/machine learning actors, e.g., identifying deep fakes Machine Learning Formulation and Evaluation, Deep Learning, RL and Ethics, Introduction to AI: Concepts and Intelligent Behavior, Problem Characteristics and Agent Nature, Machine Learning Fundamentals, Machine Learning Data, Representations and Evaluation, Neural Networks and Ethics, Civil Liberties and Expression, Data, Surveillance and Privacy Technology, Privacy Philosophical Foundations and Legislation, Computer Crimes and Attacks, Security Laws, Policies and Responsibility. • Societal impacts of Internet of Things (IoT) devices and other emerging technologies on security and privacy Civil Liberties and Expression, Data, Surveillance and Privacy Technology, Privacy Philosophical Foundations and Legislation, Computer Crimes and Attacks, Security Laws, Policies and Responsibility.	• Calculate the impact of a breakdown in security of a given system [Calculate] • Construct a system that conforms to security laws [Create] • Apply a set of privacy regulations to design a system that protects privacy [Apply] • Evaluate the legal ramifications of a system not corresponding to applicable laws and regulations [Evaluate]
Readings : [**Anderson2020**], [**Pfleeger2015**]	

8. WORKPLAN

8.1 Methodology

Individual and team participation is encouraged to present their ideas, motivating them with additional points in the different stages of the course evaluation.

8.2 Theory Sessions

The theory sessions are held in master classes with activities including active learning and roleplay to allow students to internalize the concepts.

8.3 Practical Sessions

The practical sessions are held in class where a series of exercises and/or practical concepts are developed through

problem solving, problem solving, specific exercises and/or in application contexts.

9. EVALUATION SYSTEM

********* EVALUATION MISSING ********

10. BASIC BIBLIOGRAPHY