Amrita School of Computing, Amritapuri Campus

Amrita Vishwa Vidyapeetham

Course Plan- Feb - June 2025

19CSE314 COMPUTER SECURITY L-T-P-C:2-0-3-3

S6 BTech CSE(AIE)

1. Course Information

Course Code	19CSE314	**Title**	Computer Security
Academic Year	2024– 2025	**Semester**	VI
Program	2022 BTech CSE(AIE)	**L – T – P – C**	2 – 0 – 3 – 3

2. Faculty Information

Name : **Dr.Remya. S ,** Assistant Professor, Department of CSE, ASC, Amritapuri

Email : **remyas@am.amrita.edu**

Contact No: 9447746568

Course Mentor: Dr. Remya S

3. Course Objectives

- This course provides basic knowledge and skills in the fundamental theories and practices of cyber security.
- This course provides an overview of the field of security and assurance emphasizing the need to protect information being transmitted electronically

4. Course Learning Outcomes (CO)

#CO	Outcome
CO1	Implement cryptographic techniques in secure application development.
CO2	Apply methods for authentication, access control, intrusion detection and prevention.
CO3	Apply fundamental security principles to analyze threat situations.
CO4	Design mechanisms to provide security in a network.

Program Outcomes (PO) and Program Specific Outcomes (PSO)

Program Outcomes	Objective
PO1(Engineering knowledge)	Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems
PO2(Problem analysis)	Identify, formulate, review research literature, and analyze complex engineering problems, reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3(Design/development of solutions)	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety and cultural, societal, and environmental considerations.
PO4(Numerical and Data Analysis)	Use research-based knowledge and research design of experiments, analysis and interpretation of data, and synthesis of the valid conclusion.
PO5(Modern tool usage)	Create, select and apply appropriate techniques, resources and modern including prediction and modeling to complex engineering activities with an understanding of the limitation
PO6(The engineer and society)	Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues, and the consequent responsibilities relevant to the professional engineering practice
PO7(Environment and sustainability)	Understand the impact of professional engineering solutions in societal and environmental contexts and demonstrate the knowledge of and need for sustainable development.
PO8(Ethics)	Apply ethical principles and commit to professional ethics and responsibilities and norms of engineering practice.
PO9(Individual and team work)	Function effectively as an individual and as a member or leader in diverse teams, and in multidisciplinary settings.
PO10(Communication)	Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instruction.
PO11(Project management and finance)	Demonstrate knowledge and understanding of engineering and management principles and apply these to one's own work, as a member and leader in a team. Manage projects in multidisciplinary environments.
PO12(Life-long learning)	Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Specific Outcomes (PSO)

Program Specific Outcomes	Objectives
PSO1 (Adopt Standard Practices)	Ability to design and engineer, innovative, optimal and elegant computing solutions to interdisciplinary problems using standard practices, tools and technologies.
PSO2 (Research and Innovation)	Ability to learn emerging computing paradigms for research and innovation

5. CO-PO Affinity Map

CO/ PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO1 2	PSO 1	PSO 2	PSO 3
CO 1	2	1	-	-	-	-	-	-	-	-	-	-	1	2	-
CO 2	2	2	2	-	-	-	-	-	-	-	-	-	1	2	2
CO 3	2	1	2	-	-	-	-	-	-	-	-	-	1	2	3
CO 4	2	-	-	1	-	2	-	-	-	-	-	-	1	2	-

1 – Weak affinity, 2 – Moderate affinity, 3 – Strong affinity, - No affinity

6. CO-PO Justification

CO	PO	Affinity	Justification
CO1	PO1	3	understanding basic security concepts and cryptographic methods is fundamental to applying engineering knowledge to identify and solve engineering problems.
	PO2	1	Basic comprehension is needed for problem analysis, but it's more foundational, hence the mapping is moderate.
	PO3	1	The application in design and development of solutions requires foundational knowledge of security concepts
	PSO1	1	This CO supports the ability to design and engineer computing solutions by providing the necessary foundational knowledge.
	PSO2	2	Understanding emerging paradigms in security is crucial for research and innovation, making this mapping more significant.
CO2	PO1	2	Applying cryptographic techniques directly relates to the application of engineering knowledge, though it's more specific, thus rated 2.
	PO2	2	The application involves analyzing security problems and implementing cryptographic solutions, which requires a good level of problem-solving
	PO3	1	Design and development are involved but at a more basic level for cryptographic techniques.
	PSO1	1	It supports the ability to design solutions.
	PSO1	2	Cryptographic techniques are a significant part of emerging computing paradigms, hence a stronger link.
CO3	PO1	2	This CO is important for applying engineering knowledge but more specific to security.
	PO2	1	Analyzing system and network security requires foundational problem-solving skills.
	PO3	2	The CO is more strongly linked to the design and development of security solutions, making it more critical in this context.

	PSO1	1	Supports designing computing solutions, though with a focus on analysis rather than creation.
	PSO2	2	The CO is crucial for understanding and innovating within emerging security paradigms
CO4	PO1	3	his CO is strongly aligned with applying engineering knowledge to solve real-world problems.
	PO4	1	Real-world problem-solving requires investigation and research support.
	PO6	2	Involves the use of modern security tools for problem-solving.
	PSO1	1	Supports engineering computing solutions in real-world contexts, albeit indirectly.
	PSO2	2	Choosing methodologies is key to innovation and research, particularly in applying new paradigms in security.

7. Course Syllabus

Unit 1:

Basics of Computer Security: Overview-Definition of terms-security goals-shortcomings-attack and defense-Malicious code-worms-intruders-error detection and correction.Encryption and cryptography:ciphers and codes-public key algorithm-key distribution-digital signature.

Unit 2:

Security services: Authentication and exchange protocols-Access control matrix-user authentication-directory authentication service-Diffie Hellman exchane-Kerberos.

Unit 3:

System security and security models:Disaster recovery-protection policies.Email security:Pretty good privacy-Database security:Integrity constraint-multiphase commit protocol-network security:threats in network-DS authentication-web and electronic commerce: secure socket layer-client side certificates-trusted systems:memory protection.

8. Text Book(s) and References

1. Stallings William, Cryptography and network security: Principles and practice, 7th edition, Pearson/Prentice- Hall, 2018
2. Forouzan B.A, Cryptography and network security, Special Indian edition, Tata Mc Graw Hill,2007.
3. Padmanabhan T.R.,Shyamala C.K. and Harini N, Cryptography and security, 1st edition, Wiley India Publications, 2011.

9. **Evaluation Policy: 70 (Internal Assessment) +30 (End Semester)**

a. Direct Assessment Tools

Assessment	Components	Marks	Weightage (%)
Continuous Assessment Theory (20)	Quiz1(AUMS) +Slido(Class Participation) Quiz 2(AUMS)	2*10=20 Marks	20%
Continuous Assessment Lab (30)	Assignment-1(Programming Assignment)	5 Marks	30%
	Assignment-2- Lab Sheet Submission+ Lab Viva(Written)	2+3= 5 Marks	
	Case Study (Max 4 students in a Group) ✓ Technical Analysis(5 Marks) ✓ Comparison with Existing Solutions (5 Marks) ✓ Documentation & Presentation (5 Marks) • Clear and structured report (introduction, problem statement, security measures). • Proper use of references and citations. • Well-organized presentation with diagrams/tables ✓ Viva(5 Marks)	20 Marks	
Mid-Term Examination		50 Marks	20%
End Semester Examination		100 Marks	30%

b. Indirect Assessment Tools

Course Exit Survey

c. Mode of conduct of evaluations

Evaluation	Mode of conduct
Periodicals and End semester	Periodicals and End semester exams will be conducted in the examination hall. The exam consists of questions based on real case scenarios and security related problems.
Quiz	Online quizzes conducted through AUMS during lab sessions.
Assignment	Programming or Written assignments ,test the understanding of theoretical concepts and ability to apply them to cybersecurity scenarios
Case Study	Case studies will be conducted as group work, focusing on analyzing specific cybersecurity scenarios. However, the

	presentation and viva will be conducted individually. Each student must present one algorithm, technology, or method related to the case study
Exit survey	Online survey

d. Rubrics

1) Assignment Rubrics

i. Rubrics for Assignment-1 (Programming Assignment) (Total: 5 Marks)

Criteria	Excellent	Good	Satisfactory	Needs Improvement
Implementation (3 Marks)	**3 Marks** - Code is well-structured, follows correct logic, and meets all requirements.	**2 Marks** - Code is mostly correct but has minor logical issues or inefficiencies.	**1 Mark** - Code has significant logical errors but attempts to meet requirements.	**0 Marks** - Code is incomplete, incorrect, or lacks proper implementation.
Functionality (2 Marks)	**2 Marks** - Code runs correctly and produces the expected output without errors.	**1.5 Marks** - Code runs with minor issues but mostly meets the expected output.	**1 Mark** - Code runs but has significant output errors or missing key features.	**0 Marks** - Code does not run or produces incorrect output.

ii. Rubrics for Assignment-2 (Lab Sheet Submission + Lab Viva [Written]) (Total: 5 Marks)

Criteria	Excellent	Good	Satisfactory	Needs Improvement
Lab Sheet Submission (2 Marks)	**2 Marks** - Fully completed, accurate, well-organized, and neatly presented.	**1.5 Marks** - Mostly complete with minor errors or missing details.	**1 Mark** - Partially completed with some errors or gaps in content.	**0 Marks** - Incomplete or missing.
Lab Viva (Written) (3 Marks)	The marks for the Lab Viva will be directly based on the student's performance in the written exam			

2) Rubrics for Case Study Evaluation (20 Marks)

Criteria	Excellent (5 Marks)	Good (4 Marks)	Satisfactory (3 Marks)	Needs Improvement (2 or Below Marks)
Technical Analysis (5 Marks)	Provides an in-depth analysis of threats, vulnerabilities, and mitigation strategies with clear technical details.	Covers major threats and security measures but lacks depth in some areas.	Discusses security aspects but misses key technical details or explanations.	Limited or incorrect technical analysis, lacks clarity and depth.
Comparison with Existing Solutions (5 Marks)	Compares the case study with multiple existing solutions (minimum 4), highlighting strengths, weaknesses, and improvements.	Provides a comparison but lacks a deep analysis of advantages and limitations.	Basic comparison with few details on how the solution differs.	Very Minimal or no comparison, lacks insight into alternative approaches.
Documentation & Presentation (5 Marks)	Well-structured, clear, and concise documentation with appropriate references, diagrams, and formatting.	Organized documentation with minor formatting or clarity issues.	Report is somewhat structured but lacks clarity, coherence, or proper references.	Poorly organized, unclear documentation with missing details and formatting errors.
Viva (5 Marks)	Demonstrates deep understanding, explains security concepts clearly, and answers questions confidently.	Shows good understanding but struggles slightly with some explanations.	Basic understanding but unable to elaborate on key aspects.	Limited knowledge, unable to answer questions clearly.

10. Direct Assessment Tools

Sl. No	Direct Assessment Tools	Weightage	CO wise mark distribution			
			CO1	CO2	CO3	CO4
1	Midterm	20	✓	✓		✓
2	Quiz 1	10	✓			
3	Quiz 2	10		✓		
4	Assignment 1	5			✓	
5	Assignment 2	5	✓	✓	✓	✓
6	Case Study	20			✓	
7	End Semester	30	✓	✓	✓	✓

11. Threshold and Target

CO	Threshold%	Target%
CO1	60	60
CO2	60	60
CO3	60	60
CO4	60	60

12. Course Outcome Attainment Levels

Since the course is offered for the first time, 60 (out of 100) is set as threshold for all course outcomes.

The target levels are given below.

Attainment Level	Target %
High	>=60
Medium	>= 40
Low	>=20
No attainment	<20

13. Course Delivery Plan

Lecture	Topics	Sub Topics	Objectives	CO mapped
Week 1: Feb 3-7	Basics of Computer security:	Course introduction, Course plan Overview, Definition of terms Security goals- key objectives-CIA Triad	Understand the fundamental concepts of Computer security	CO1
Week 2: Feb 10-15	OSI architecture	Security architecture, Security attacks, Security services Security mechanism Security Model	Understand the different security attacks and services.	CO1,CO3
Week 3: Feb 17-21	Classical Encryption Techniques	Substitution Techniques and Transposition Techniques		
Week 4: Feb 24-28	Threats to information security	Malicious code IPS,IDS	Understand how malicious attacks threats etc. affect a system's infrastructure.	CO1,CO2
Week 5: Mar 3-7	Error detection and correction	Parity bit, 2D parity check Checksum CRC	To study the different error detection and correction methods.	CO2
Week 6: Mar 10-14	Encryption and Cryptography	Ciphers and codes Public key algorithm Symmetric and asymmetric key cryptography **Quiz 1**	To introduce different models involved in encryption and cryptography.	CO2
Week 7: Mar 17-21	Public Key cryptography	RSA Algorithms		
Week 8: Mar 17-21	**Mid Term Examination**			
Week 9: Mar 24-29	Key distribution Digital signatures.	Distribution of public keys properties of digital signature	Demonstrate knowledge in term of relevance and potential of	CO4

		RSA digital signature,examples etc. **Assignment 1**	computer security for a given application.	
Week 10: Apr 1-4	Security Services	Authentication-remote user authentication Authentication protocols Key exchange protocols	To understand and apply different security services.	CO3
Week 11-15 Apr 5-May 4	Summer Vacation			
Week 16: May 6-9	Access control matrix	Access control matrix user authentication	To understand the concept of access control methods.	CO3
Week 17: May 12-16	Directory authentication service	Directory authentication service Diffie Hellman Key exchange Kerberos	Learn about directory authentication services.	CO2,CO3
Week 18: May 19-23	System security and security models	Disaster recovery - Protection policies Email security: Pretty good privacy-S/MIME **Quiz 2**	Demonstrate the knowledge of system security and security models.	CO4
Week 19: May 26-31	Database Security	Integrity constraints Access control disaster recovery Multi-phase commit protocols **Case Study Starts**	Understand how database security is done. Learn about different protocols	CO3, CO4
Week 20: June 2-5	Network Security:	Threats in networks **Assignment 2**	To get practical knowledge in network security.	CO3,CO4
Week 21: June 9-13	DS authentication	DS authentication -	Demonstrate the idea of DS authentication.	CO3

	Web and Electronic Commerce:	Secure socket layer Client-side certificates	Understand the knowledge of web security.	CO3,CO4
Week 22: June 16-18	Trusted Systems	Memory protection.	Learn about memory protection models.	CO4
REVISION				

Signature of Faculty:

Counter signed by

Class committe chair
Vice chair/Chair