College of Computer Science and Information Systems | **Department of Computer Science**

Course Code : 429CSS-3 | **Computer Security**

Contact Hour : 3(0) | **Prerequisite : 329CSS-3**

Coordinator -

2. Course Description

Introduction to Computer security and its terminology, user authentication, Security services: confidentiality, integrity, availability. security flaws and vulnerabilities. Symmetric & Asymmetric cryptography tools such as: DES, 3DES, and AES. Message authentication and protocols such as: Hash function, SHA-3. Malicious software, Denial of service attacks, intrusion detection system, firewalls, and intrusion prevention system. Internet security protocols and applications.

3. Course Learning Outcomes

SL	By the end of this course, students should be able to:	Linkages to POs
1.	Define the basic concepts and terminology of computer security.	a(S)
2.	Describe types of attacks related to computer/network systems and security services.	b(S),c(W)
3.	Distinguish symmetric and asymmetric cryptographic algorithms and their applications.	i(W),j(S)
4.	Classify user and message authentication algorithms and their applications.	i(W),j(S)
5.	Evaluate different types of malicious software, intrusion detection and prevention methods.	i(W),j(S)
6.	Illustrate the security protocols & applications devised for internet.	i(W),j(S),k(W)

4. Learning Resources

Text	William Stallings and Lawrie Brown, Computer Security Principles and Practice, Pearson/Prentice Hall, Latest Edition.
Reference	Matt Bishop, Introduction to Computer Security, Addison Wesley, Latest Edition
Reference	Charles P. Pfleeger and Shari L. Pfleeger, Security in Computing, Prentice-Hall
Reference	Stallings, W., Cryptography and Network Security: Principles and Practice, Prentice Hall

5. Course Content : The list below provides a summary of the material that will be covered during the course

Week	Topics	References Book / Others Source	Special Event	Tutorial Activities	Lab Activities
1.	Introduction to computer security concepts	Chapter 1			
2.	Cryptographic Tools	Chapter 2			
3.	User Authentication	Chapter 3	Quiz 1 (3rd week)	Tutorial 1	Lab Activity 1
4.	Symmetric encryption & message confidentiality	Chapter 19	Assignment 1 (5th week)	Tutorial 2	Lab Activity 2,3
5.	Public key cryptography	Chapter 20	Midterm Exam-I		Lab Activity 4
6.	Hash Algorithms	Chapter 20	Lab Assignment 1 (7th week)	Tutorial 3	Lab Activity 5
7.	Key management & distribution	Chapter 20 & 19	Quiz 2 (8th week)		Lab Activity 6
8.	Internet security protocols	Chapter 21	Assignment 2 (9th week)	Tutorial 4	Lab Activity 7

9.	Internet authentication applications	Chapter 22	Midterm Exam-II		Lab Activity 8,9
10.	Intrusion detection	Chapter 6	Lab Assignment 2 (11th week)	Tutorial 5	Lab Activity 10
11.	Intrusion prevention	Chapter 9			Lab Activity 11
12.	Honeypots, SNORT	Chapter 9		Tutorial 5	
13.	Malicious software	Chapter 7	Quiz 3 (13th week)		Lab Activity 12
14.	Firewalls	Chapter 8 ,9	Final Lab Exam		

6. Evaluation Scheme: The following list is the contribution of course components to the final grade for the course.	
Component	Weight (%)
Quizzes	5
Assignment 1	5
Mid Term 1	15
Mid Term 2	15
Lab Performance and Exam	10
Lab Final	10
Final Exam	40
Total	100