COURSE NAME: **Network and Data Security**
(A Program Elective for CSE students) L-T-P-C: 3 - 1 - 0 - 4

1. OUTLINE:

This course introduces the concepts of network security and data security to students. It develops a basic understanding of various network and distributed system attacks, and their respective defenses mechanisms. The introduction of various cryptographic techniques and tools is also a part of this course. The students will learn about the authentication and access control methods and also be introduced the concept of web application security. The projects and assignments part of this course is meant to introduce various security tools to students. Overall, the course will be helpful for the students in designing effective network and data defense approaches for different networks.

2. OBJECTIVES:

At the end of this course, the students will be able to:

- identify security requirements and security risks.
- apply different security mechanisms to counter the identified security and privacy risks.
- design effective defense methods against various attacks targeting network and data security
- identify several encryption and decryption techniques for implementing data security.
- classify network infrastructure, end-to-end identity and access management in cloud.
- understand various web application security methods and tools.

3. PRE-REQUISITES:

Basics of Computer Networks.

4. COURSE OUTLINE (TOPICS):

The following list of topics is tentative.
Based on available time slots, some topics may be dropped or added or reordered.

Chapter 1 Overview

1.1 Security Concepts
1.2 Threats, Attacks, and Assets
1.3 Security Functional Requirements

1.4 Fundamental Security Design Principles
1.5 Attack Surfaces and Attack Trees
1.6 Security Strategy

Part 1 Network Security

Chapter 2 Network Attacks
2.1 MITM
2.2 DoS/DDoS
2.3 ARP Spoofing
2.4 IP Spoofing
2.5 DNS Spoofing
2.6 Other Attacks

Chapter 3 Intrusion Detection and Prevention
3.1 Intruders
3.2 Intrusion Detection
3.3 Analysis Approaches
3.4 Host-Based Intrusion Detection
3.5 Network-Based Intrusion Detection
3.6 Distributed or Hybrid Intrusion Detection
3.7 Firewalls
3.8 The Need for Firewalls
3.9 Firewall Characteristics and Access Policy
3.10 Types of Firewalls
3.11 Intrusion Prevention Systems

Part 2 Data Security

Chapter 4 Cryptographic Tools
4.1 Confidentiality, Integrity, Authentication (CIA)
4.2 Symmetric Encryption
4.3 Message Authentication and Hash Functions
4.4 Public-Key Encryption
4.5 Digital Signatures
4.6 Digital Envelope

Chapter 5 User Authentication and Access Control
5.1 Electronic User Authentication Principles
5.2 Password-Based Authentication
5.3 Token-Based Authentication
5.4 Biometric Authentication
5.5 Access Control Principles
5.6 Subjects, Objects, and Access Rights
5.7 Discretionary Access Control
5.8 Role-Based Access Control

5.9 Attribute-Based Access Control

Part 3 Web Application Security

Chapter 6 Web Application Security
6.1 Three Tier Architecture of Web Applications
6.2 SQL Injection, XSS and CSRF
6.3 Session Management
6.4 Other vulnerabilities at the application layer

5. TENTATIVE WEEKLY PLAN

Module	Week	Topics Scheduled to be Covered
1	1	Security Concepts, Threats, Attacks, and Assets, Security Functional Requirements, and Fundamental Security Design Principles
	2	Attack Surfaces and Attack Trees and Security Strategy
2	3	MITM, DoS/DDoS, and ARP Spoofing
	4	IP Spoofing, DNS Spoofing, and Other Attacks
3	5	Intruders, Intrusion Detection, Analysis Approaches, Host-Based Intrusion Detection, Network-Based Intrusion Detection
	6	Distributed or Hybrid Intrusion Detection, Firewalls, Intrusion Prevention Systems
4	7	Confidentiality, Integrity, Authentication (CIA), Symmetric Encryption, Message Authentication and Hash Functions
	8	Public-Key Encryption, Digital Signatures, Digital Envelope
5	9	Electronic User Authentication Principles, Password-Based Authentication, Token-Based Authentication, Biometric Authentication
	10	Access Control Principles, Discretionary Access Control, Role-Based Access Control, Attribute-Based Access Control
6	11	Three Tier Architecture of Web Applications, SQL Injection, XSS and CSRF
	12	Session Management, Other vulnerabilities at the application layer

6. BOOKS:

TEXT BOOKS:

- William Stallings and Lawrie Brown. Computer Security Principles and Practice (3rd Edition), Pearson, 2014
- William Stallings, “Cryptography and Network Security, Principles and Practices”, Pearson Education, Third Edition

Reference Books

- "The web application hacker's handbook: Finding and exploiting security flaws" by Stuttard and Pinto
- Robert Bragge, Mark Rhodes, Heith straggberg, "Network Security the Complete Reference", Tata McGraw Hill Publication.

6. COURSE GRADING - EVALUATION COMPONENTS:

Course grades will be based on the following tentative weightage pattern.

a) EXAMINATIONS: 50%
Mid Semester Exam: 20%
End Semester Exam: 30%

b) RESEARCH WORK / TAKE HOME ASSIGNMENTS: 25%

This evaluation component consists of practical assignments where students will learn different security tools. Additionally, students will also be asked to read/implement latest research papers in this area.

c) CLASS PARTICIPATION (SURPRISE QUIZZES): 10%

This evaluation component will consist of surprise tests conducted during class hours.

d) SCHEDULED QUIZZES: 15%

This evaluation component will consist of announced quizzes which will test the students' comprehension of the topics covered in class

7. ETHICS:

Please note down the following activities leading to a fair academic honesty:

a) All class work is to be done independently.
b) It is best to try to solve problems on your own, since problem solving is an important component of the course, and exam problems are often based on the outcome of the assignment problems.
c) You are allowed to discuss class material, assignment problems, and general solution strategies with your classmates. But, when it comes to formulating or writing solutions you must work alone.
d) You may use free and publicly available sources, such as books, journal and conference

publications, and web pages, as research material for your answers. (You will not lose marks for using external sources.)

e) You may not use any paid service and you must clearly and explicitly cite all outside sources and materials that you made use of.

f) The use of uncited external sources as portraying someone else's work as your own is a violation of the University's policies on academic dishonesty.

g) Such Instances will be dealt with harshly and typically result in a failing course grade.