Subject Name : Information Security

Subject Code : IT 502

Teaching Scheme (Credits and Hours)

Teaching scheme				Total Credit	Evaluation Scheme					
L	T	P	Total		Theory		Mid Sem Exam	CIA	Pract.	Total
Hrs	Hrs	Hrs	Hrs		Hrs	Marks	Marks	Marks	Marks	Marks
04	00	02	06	5	3	70	30	20	30	150

Learning Objectives:

- Learn fundamentals of cryptography and its application to network security.
- Understand network security threats, security services, and countermeasures.
- Understand vulnerability analysis of network security.
- Acquire background on hash functions; authentication; firewalls; intrusion detection techniques.
- Gain hands-on experience with programming and simulation techniques for security protocols.
- Obtain background for original research in network security, especially wireless network and MANET security.
- Understand the tradeoffs and criteria/concerns for security countermeasure development.
- Apply methods for authentication, access control, intrusion detection and prevention.
- Indentify and mitigate software security vulnerabilities in existing systems.

Outline of the Course:

Sr. No	Title of the Unit	Minimum Hours
1	Introduction to Information Security	5
2	Conventional Cryptographic Techniques	10
3	Symmetric and Asymmetric Cryptographic Techniques	10
4	Authentication and Digital Signatures	9
5	Program Security	12
6	Security in Networks	14

Total hours (Theory): 60

Total hours (Lab): 30

Total hours: 90

Detailed Syllabus

Sr. No	Topic	Lecture Hours	Weightage(%)
1	Introduction to Information Security : Attacks, Vulnerability, Security Goals, Security Services and mechanisms	5	8
2	Conventional Cryptographic Techniques : Conventional substitution and transposition ciphers, One-time Pad, Block cipher and Stream Cipher, Steganography	10	17
3	Symmetric and Asymmetric Cryptographic Techniques : DES, AES, RSA algorithms	10	17
4	Authentication and Digital Signatures : Use of Cryptography for authentication, Secure Hash function, Key management – Kerberos	9	15
5	Program Security : Nonmalicious Program errors – Buffer overflow, Incomplete mediation, Time-of-check to Time-of-use Errors, Viruses, Trapdoors, Salami attack, Man-in-the-middle attacks, Covert channels	12	20
6	Security in Networks : Threats in networks, Network Security Controls – Architecture, Encryption, Content Integrity, Strong Authentication, Access Controls, Wireless Security, Honeypots, Traffic flow security, Firewalls – Design and Types of Firewalls, Personal Firewalls, IDS, Email Security – PGP,S/MIME	14	23
	Total	**60**	**100**

Instructional Method and Pedagogy:

- At the start of course, the course delivery pattern, prerequisite of the subject will be discussed.
- Lectures will be conducted with the aid of multi-media projector, black board, OHP etc.
- Attendance is compulsory in lecture and laboratory which carries 10 marks in overall evaluation.
- One internal exam will be conducted as a part of internal theory evaluation.
- Assignments based on the course content will be given to the students for each unit and will be evaluated at regular interval evaluation.
- Surprise tests/Quizzes/Seminar/tutorial will be conducted having a share of five marks in the overall internal evaluation.
- The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
- Experiments shall be performed in the laboratory related to course contents.

Learning Outcome:

After completion of the course, students should be able to:

- Understand and explain the risks faced by computer systems and networks.
- Identify and analyze security problems in computer systems and networks.
- Explain how standard security mechanisms work.
- Develop security mechanisms to protect computer systems and networks.
- Write programs that are more secure.
- Use cryptography algorithms and protocols to achieve computer security.

Reference Books:

1. Security in Computing, Fourth Edition, by Charles P. Pfleeger, Pearson Education
2. Cryptography And Network Security Principles And Practice, Fourth or Fifth Edition, William Stallings, Pearson
3. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall.
4. Network Security Essentials: Applications and Standards, by William Stallings. Prentice Hall.

List of experiments:

Sr. No.	Name of Practical
01	Implement Ceaser Cipher
02	Implement Affine Cipher with equation c=3x+12
03	Implement Playfair Cipher with key entered by user.
04	Implement polyalphabetic Cipher
05	Implement AutoKey Cipher
06	Implement Hill Cipher.
07	Implement Rail fence technique
08	Implement Simple Columner Transposition technique
09	Implement Advanced Columner Transposition technique.
10	Implement Simple RSA Algorithm with small numbers.
11	Implement Simplified DES
12	Make a study of one IDS (For ex. Snort)