Information Security(PCCS5030T)

Teaching Scheme
Lectures : 03 Hrs./week
Credits : 03

Examination Scheme
Term Test : 15 Marks
Teacher Assessment : 20 Marks
End Sem Exam : 65 Marks
Total Marks : 100 Marks

Prerequisite: Computer Basics.

Course Objectives: The objective of the course is to introduce indicators of system security, recognize various threats, attacks and vulnerabilities.

CO	Course Outcomes	Blooms Level	Blooms Description
CO1	Understand system security goals and concepts, classical encryption techniques and acquire fundamental knowledge on the concepts of modular arithmetic and number theory.	L2	Understand
CO2	Understand, compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication.	L2, L3, L5	Understand, Compare, Apply
CO3	Apply the knowledge of cryptographic checksums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes.	L3, L5	Apply, Evaluate
CO4	Apply different digital signature algorithms to achieve authentication and design secure applications.	L3	Apply
CO5	Understand network security basics, analyze different attacks on networks and systems.	L2, L4	Understand, Analyze
CO6	Understand Software vulnerability and Apply preventive measures.	L2, L3	Understand, Apply

R. C. Patel Institute of Technology, Shirpur
SES
Autonomous

Course Contents

Unit-I Introduction — 10 Hrs.

Introduction: Cyber Attacks, Need of Security, Security Approaches, Principles of security (confidentiality, authentication, integrity, non-repudiation, access control availability), types of attacks.

Networking Basics: Local Area Network, Protocols - Network Layer, Transport Layer and Application Layer.

Unit-II Number Theory — 06 Hrs.

Modulo Arithmetic, Euclid's Algorithm, Fermat's and Euler's Theorem, Chinese Remainder Theorem, Cipher Properties, Substitution Ciphers – Monoalphabetic Ciphers, Polyalphabetic Ciphers, Transposition Ciphers.

Unit-III Symmetric Cryptography — 08 Hrs.

Block Cipher, Fiestel Structure, Block Cipher Modes of Operation, S-DES, Double DES, Triple DES, AES Algorithm.

Unit-IV Asymmetric Cryptography — 06 Hrs.

Private Key and Public Key Cryptography, The RSA algorithm, Key Management, Diffie-Hellman Key Exchange, Elliptic Curve Operations, Elliptic Curve Diffie-Hellman (ECDH) Key Exchange Algorithm.

Unit-V Integrity and Authentication — 06 Hrs.

Hashing: Properties of cryptographic hash, message digest, MD-5, SHA-1. Public Key Infrastructure (PKI), One way and mutual authentication, Needham-Schroeder Protocol, Authentication methods, Kerberos Authentication Protocol, Biometrics, Digital Certificates: X.509.

Unit-VI Network Security — 06 Hrs.

Network attacks, DoS and DDoS attack, Sniffing, Session hijacking, Spoofing, Phishing, Cross-site Scripting (XSS), IPSec Protocol, SSL Handshake Protocol, Firewalls, IDS Prevention and Detection.

Text Books:

1. William Stallings, "Crpyptography and Network Security Principles and Practices", 7th Edition, Pearson Education, 2017.

2. Behrouz A. Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", 3rd Edition, McGraw Hill, 2015.

R. C. Patel Institute of Technology, Shirpur
SES
Autonomous

Reference Books:

1. Atul Kahate, "Cryptography and Network Security", 3rd Edition, McGraw Hill, 2017.
2. Bernard Menezes, "Network Security and Cryptography", 1st Edition, Cengage Learning, 2010.
3. Wade Trappe, Lawrence C Washington, "Introduction to Cryptography with coding theory", 2nd Edition, Pearson, 2005.
4. W. Mao, "Modern Cryptography, "Theory and Practice", 1st Edition, Pearson Education, 2003.
5. Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, "Security in computing", Pearson, 5th Edition, 2015.

Web Links:

1. Damn Vulnerable Web Application (DVWA): http://dvwa.co.uk
2. Open Web Application Security Project: https://owasp.org
3. Web penetration testing: https://pentesterlab.com
4. Penetration Testing: https://kali.org

Evaluation Scheme:

Theory :

Continuous Assessment (A):

Subject teacher will declare Teacher Assessment criteria at the start of semester.

Continuous Assessment (B):

1. Two term tests of 15 marks each will be conducted during the semester.
2. Average of the marks scored in both the tests will be considered for final grading.

End Semester Examination (C):

1. Question paper based on the entire syllabus, summing up to 65 marks.
2. Total duration allotted for writing the paper is 3 hrs.

R. C. Patel Institute of Technology, Shirpur
SES
SHIRPUR EDUCATION SOCIETY
Autonomous

Information Security Laboratory (PCCS5030L)

Practical Scheme
Practical : 02 Hrs./week
Credit : 01

Examination Scheme
Teacher Assessment : 25 Marks
End Sem Exam : 25 Marks
Total : 50 Marks

Course Objectives:

1. Apply the cryptographic algorithms for data communication.
2. Demonstrate the data integrity using various cryptographic algorithms.
3. Implement Digital signature for secure data transmission
4. Utilize the different open source tools for network security and analysis.
5. Demonstrate Network Intrusion Detection using network security tool.

CO	Course Outcomes	Blooms Level	Blooms Description
CO1	Apply the cryptographic algorithms for data communication.	L3	Apply
CO2	Demonstrate the data integrity using various cryptographic algorithms.	L2, L3	Understand, Apply
CO3	Implement Digital signature for secure data transmission.	L6	Create
CO4	Utilize the different open source tools for network security and analysis.	L3	Apply
CO5	Demonstrate Network Intrusion Detection using network security tool.	L2, L3	Understand, Apply

R. C. Patel Institute of Technology, Shirpur
SES
Autonomous

List of Laboratory Experiments

Suggested List of Experiments:

1. Create a network using CISCO packet tracer.
2. Connect the computers in Local Area Network.
3. Implement Playfair Cipher with key entered by user.
4. Implement polyalphabetic Cipher.
5. Implement Simple and Advanced Columnar Transposition technique.
6. Implement Simplified DES.
7. Implement Simple RSA Algorithm with small numbers.
8. Implement Diffie-Hellman Key Exchange.
9. Implement DoS and DDoS attack using Hping.
10. Implement phishing attack using HTTrack Website Cloning.
11. Implement static code analysis using Flawfinder Python Distribution.
12. Implement packet sniffing using Wireshark and TCP Dump.
13. Implement cross site request forgery in a controlled virtual environment using DVWA Web Server.
14. Implement firewalls using IP tables.
15. Implement Network Intrusion Detection System (NIDS).
16. Implement Host based Intrusion Detection System (HIDS).

Any other experiment based on syllabus may be included, which would help the learner to understand topic/concept.

Evaluation Scheme:

Laboratory:

Continuous Assessment (A):

Laboratory work will be based on PCCS5030T with minimum 10 experiments to be incorporated. The distribution of marks for term work shall be as follows:

1. Performance in Experiments: 05 Marks

R. C. Patel Institute of Technology, Shirpur
SES
SHIRPUR EDUCATION SOCIETY
Autonomous

2. Journal Submission: 05 Marks

3. Viva-voce: 05 Marks

4. Subject Specific Lab Assignment/Case Study: 10 Marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work and upon fulfilling minimum passing criteria in the term work.

End Semester Examination (C):

Oral/ Practical examination will be based on the entire syllabus including, the practicals performed during laboratory sessions.

R. C. Patel Institute of Technology, Shirpur
SES
SHIRPUR EDUCATION SOCIETY
Autonomous