CM31234A: INFORMATION SECURITY

Teaching Scheme	Examination Scheme				
Credits: 04 **Lecture (L):** 03hrs / week **Laboratory(L):**02 hours /Week	CIE	SCE	PR/OR	ESE	Total
	20	20	20	40	100

Prerequisite: Linear Algebra, Computer networks

Course objectives: After completion of the course, student will be able to

1. To understand the core principles of information security
2. To compare and evaluate different authentication techniques and access control models used to ensure secure system access.
3. To comprehend and apply classical cryptographic techniques.
4. To explore and demonstrate the working of cryptographic hash functions and digital signature algorithms.
5. To illustrate the working of Internet security mechanisms
6. To recognize different types of cybercrimes and classify them based on legal categories

Course Outcomes:

Upon completion of the course, students will be able to:

1. Understand the foundational concepts and significance of information security.
2. Analyze various user authentication methods, and access control mechanisms to ensure system authorization.
3. Understand the fundamental concepts of cryptography
4. Explore the hashing and digital signature techniques.
5. Understand key Internet security protocols
6. Identify and categorize cyber offenses against individuals, property, and government.

Contents

Unit I – Introduction to Information Security (4 hrs)

Security Goals, Elements of information security, Security Policy, Security Attacks, Security Mechanism, Security Services, OSI Security, Application Security, A Model for Network Security.

Unit II – User Authentication and Access Control (8 hrs)

Identification and Authentication methods: Electronic user authentication, username and password, multi-factor authentication, token-based authentication, biometrics Guessing password, Password attacks: Piggybacking, Shoulder surfing, Dumpster diving Biometrics : Finger prints, Hand prints, Retina scan patterns, Voice patterns Authorization : Introduction to authorization, goals of authorization Access controls : Access control principles, Access rights and permission Access control policies : Discretionary access control (DAC), Mandatory access control (MAC), Role-based access control (RBAC), Attribute-based access control (ABAC)

Unit III –Fundamentals of Cryptography	**(6 hrs)**
Introduction: Plain text, Cipher text, Cryptography, Cryptanalysis, Cryptology, Encryption, Decryption, Symmetric and Asymmetric cryptography: Introduction, working, key management, asymmetric cryptography -public key distribution, Substitution techniques: Caesar cipher, Playfair cipher, Hill cipher, Polyalphabetic Ciphers , Vernam cipher (One-time pad), Transposition techniques: Rail fence technique, Simple columnar technique, Block Ciphers and Data Encryption standards Steganography: Introduction and working of steganography	
Unit IV–Encryption Algorithms	**(6 hrs)**
DES (Data Encryption Standard) algorithm, AES (Advanced Encryption Standard) algorithm, RSA algorithm, Diffie-Hellman key exchange algorithm, Man-in-middle attack, Hash Function: Introduction, Features of Hash Functions, MD5 and SHA algorithm. Message Authentication Codes: Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs. Digital Signature: Introduction and working of digital signature, Threats to mobile phone and its security measures.	
Unit V: Internet Security	**(6 hrs)**
IP Sec Protocol, SSL Protocol, Firewall : Need of firewall, Types of firewalls : Packet filters, Stateful packet filters, Application gateways, Circuit gateways, Firewall policies: Configuration, Limitations, Demilitarized zone (DMZ), Intrusion Detection System(IDS) : Network-based IDS, Host-based IDS, Honeypots, E-mail security : Simple mail transfer protocol (SMTP), Pretty good privacy (PGP), S/MIME, VPN, Security maintenance, Concepts of trusted system, Trusted computing.	
Unit VI: Cyber Laws	**(6 Hrs)**
Cybercrime: Introduction, Hacking, Digital forgery, Cyber stalking/Harassment, Cyber pornography, Identity theft & fraud, Cyber terrorism, Cyber defamation, OS fingerprinting, Cyber Laws: Introduction, Need, Categories: Crime against individual, Government, Property, The Indian IT Act-Challenges, Amendments, Challenges to Indian Law and Cybercrime Scenario in India, Indian IT Act.	
Textbooks:	
1. Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson Education. 2. Forouzan, B. A., & Mukhopadhyay, D. (2010). *Cryptography and network security* (3rd ed.). McGraw-Hill Education.	
Reference books:	
1. Whitman, M. E., &Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning. 2. Stallings, W., & Brown, L. (2015). *Computer security: Principles and practice* (3rd ed.). Pearson. 3. Bidgoli, H. (Ed.). (2006). Handbook of information security: Threats, vulnerabilities, prevention, detection and management. Wiley.	
List of Assignments:	

1. Write a Python program to encrypt and decrypt text using the Play fair Cipher, Vignere Cipher, Simple columnar technique and Rail fence technique
2. Write Python program to encrypt and decrypt text using the AES algorithm
3. Write a Python program to encrypt a message using RSA. Explain the concept of public and private keys.
4. Implement MD5 Hashing: Calculate the MD5 message digest of a text input using Java.
5. Network Scanning Using Nikto: A Practical Approach to perform network discovery and scanning Using Nikto.
6. Use Burp Suite to perform a basic security assessment of a dummy web application. Identify vulnerabilities like XSS or SQL injection.
7. Conduct a vulnerability scan on a virtual machine using Nessus. Identify vulnerabilities and suggest fixes.
8. Configure and demonstrate use of vulnerability assessment tool like Wireshark or SNORT
9. Implement cryptographic watermarking for an image in Python
10. Case study about Cyber Laws, Digital Watermarking, IP Security Protocol, Digital Forgery and Cyber defamation.

Mini Project 1: SQL Injection attacks and Cross -Site Scripting attacks are the two most common attacks on web application. Develop a new policy-based Proxy Agent, which classifies the request as a scripted request or query-based request, and then, detects the respective type of attack, if any in the request. It should detect both SQL injection attack as well as the Cross-Site Scripting attacks.

OR

Mini Project 2: This task is to demonstrate insecure and secured website. Develop a web site and demonstrate how the contents of the site can be changed by the attackers if it is http based and not secured. You can also add payment gateway and demonstrate how money transactions can be hacked by the hackers. Then support your website having https with SSL and demonstrate how secured website is.

List of NPTEL/MOOC Courses

1.Information Security and Cyber Laws by Prof. S. R. Biradar, IIT Kharagpur
https://nptel.ac.in/courses/106/106/106106193/

2.Cryptography and Network Security, by Prof. Manoj Kumar, IIT Roorkee
https://nptel.ac.in/courses/106/104/106104114/