INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

<table>
<tr><th colspan="9">SECURITY PROTOCOLS LABORATORY</th></tr>
<tr><td colspan="9">VII Semester: CSE | IT</td></tr>
<tr><td>Course Code</td><td>Category</td><td colspan="3">Hours/Week</td><td>Credits</td><td colspan="3">Maximum Marks</td></tr>
<tr><td rowspan="2">ACSD55</td><td rowspan="2">Core</td><td>L</td><td>T</td><td>P</td><td>C</td><td>CIA</td><td>SEE</td><td>Total</td></tr>
<tr><td>0</td><td>0</td><td>2</td><td>1</td><td>40</td><td>60</td><td>100</td></tr>
<tr><td>Contact Classes: Nil</td><td>Tutorial Classes: Nil</td><td colspan="4">Practical Classes: 45</td><td colspan="3">Total Classes: 45</td></tr>
<tr><td colspan="9">Prerequisite: Basic knowledge of Computer Networks, Operating Systems, and Cryptography.</td></tr>
</table>

I. COURSE OVERVIEW:

This course deals with the practical understanding and implementation of security protocols used in computer networks and distributed systems. The laboratory focuses on hands-on experience in cryptographic mechanisms, authentication protocols, secure communication protocols, and network security protocols. Students will gain the ability to analyze protocol behavior, identify vulnerabilities, and implement secure communication systems. The course bridges theoretical security concepts with real-world applications through simulations, packet analysis, and protocol implementations.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The fundamentals of cryptographic algorithms and key management techniques.

II. The working principles of authentication and secure communication protocols.

III. The implementation and analysis of network and web security protocols.

IV. The use of security tools for protocol analysis and secure application development.

III. COURSE OUTCOMES:

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

CO 1 Demonstrate the use of cryptographic techniques for ensuring confidentiality, integrity, and authentication in data communication.

CO 2 Implement secure authentication and key exchange mechanisms for protected system access.

CO 3 Examine secure communication protocols through packet inspection and protocol tracing tools.

CO 4 Identify security weaknesses in protocols and demonstrate appropriate countermeasures against common attacks.

CO 5 Develop secure applications by integrating standard security protocols and best practices.

CO 6 Compare the effectiveness of various network, web, and wireless security protocols in real-world scenarios.

IV. COURSE CONTENT:

Week-l: LAB ORIENTATION AND SECURITY TOOLS
Introduction to security protocols, Linux operating environment, OpenSSL, Wireshark, and basic security commands.

Week-2: CRYPTOGRAPHIC FUNDAMENTALS
Implementation of symmetric and asymmetric encryption techniques (AES, RSA) and hash functions using OpenSSL.

Week-3: KEY MANAGEMENT AND DIGITAL CERTIFICATES
Generation of public-private key pairs, creation of digital certificates, certificate authorities, and verification mechanisms for secure communication.

Week-4: SECURE SOCKET LAYER / TLS PROTOCOL
Study of SSL/TLS handshake process, cipher suites, and packet capture with analysis using Wireshark for secure communication.

Week-5: AUTHENTICATION PROTOCOLS
Implementation of password-based authentication and challenge-response mechanisms to ensure secure user verification.

Week-6: KERBEROS AUTHENTICATION PROTOCOL
Study of Kerberos architecture and simulation of ticket-based authentication process for secure network access.

Week-7: SECURE EMAIL PROTOCOLS
Implementation of PGP-based email encryption, digital signing, and verification techniques for secure email communication.

Week-8: SECURE FILE TRANSFER PROTOCOLS
Implementation and comparison of secure file transfer mechanisms such as SFTP, SCP, and FTPS.

Week-9: NETWORK SECURITY PROTOCOLS
Study and simulation of IPsec architecture including AH, ESP, and VPN-based secure communication.

Week-10: WEB SECURITY PROTOCOLS
Implementation of HTTPS, secure cookies, and basic OAuth authentication flow for securing web applications.

Week-11: WIRELESS SECURITY PROTOCOLS
Study and analysis of wireless security standards WEP, WPA, WPA2, WPA3, and IEEE 802.1X authentication mechanisms.

Week-12: SECURE MESSAGING PROTOCOLS
Implementation of end-to-end encrypted messaging techniques with verification of integrity and confidentiality.

Week- 13: SECURITY ATTACKS AND PROTOCOL ANALYSIS
Demonstration and analysis of replay attacks, man-in-the-middle attacks, and protocol vulnerabilities.

Week- 14: MINI PROJECT AND EVALUATION
Design and implementation of a secure application or protocol followed by project demonstration and viva voce.

IV. TEXTBOOKS:

1. William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Education.
2. Bruce Schneier, *Applied Cryptography*, Wiley Publications.

V. REFERENCE BOOKS:

1. Charlie Kaufman, Radia Perlman, Mike Speciner, *Network Security: Private Communication in a Public World*, Prentice Hall.
1. Behrouz A. Forouzan, *Data Communications and Networking*, McGraw-Hill.
2. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, *Cryptography Engineering*, Wiley.

VI. ELECTRONICS RESOURCES:

1. http://www.iare.ac.in

VII.MATERIAL ONLINE:

1. Course template
2. Lab manual