COURSE MODULE OF THE SUBJECT TAUGHT FOR THE SESSION 2025-26 - (EVEN SEM)

Course Syllabus with CO's

Faculty Name: Ms. Sandhya G			**Academic Year: 2025 - 2026**				
Department: Computer Science & Engineering - Cyber Security							
Course Code	**Course Title**	**Core / Elective**	**Prerequisite**	**Contact Hours**			**Total Hrs/ Sessions**
				L	**T**	**P**	
BCY613D	**Wireless and Mobile Device Security**	Core	Basic computer fundamentals, Familiarity with MS-Office applications.	3	0	0	40T
Course Objectives	1. Understand the evolution of wired and wireless networks and their societal and economic impacts. 2. Learn about mobile communication technologies and associated security challenges. 3. Analyse WLAN fundamentals, vulnerabilities, and threat scenarios. 4. Explore security measures for WLANs and mobile devices. 5. Gain proficiency in risk assessment and security tools for wireless networks.						
Topics Covered as per Syllabus							
Module-1							
Evolution of Data and Wired Networking **The Evolution of Data Networks:** The Dawn of Data Communication; Early Data Networks; The Internet Revolution; Advances in Personal Computers and Mobile Phones; Computers Go Mobile; Convergence of Mobile and Data Networks; Business Challenges Addressed by Wireless Networking; IP Mobility and BYOD Impact; Security Considerations and Cybercrime Evolution; **The Evolution of Wired Networking to Wireless Networking:** Networking and OSI Reference Model; Layers of the OSI Model; Transition from Wired to Wireless Networking; Economic Impact of Wireless Networking; Applications in Health Care, Warehousing, Retail, and Knowledge Work; WiFi Impact on Developing Nations and IoT Introduction							
Module-2							
The Mobile Revolution and Security Threats The Mobile Revolution: Cellular Communication and Coverage; Frequency Sharing and Handoff; Evolution of Mobile Networks (1G to 4G/LTE); BYOD and Economic Impact of Mobility; Business Use Cases for Mobile Networking;							

Security Threats Overview: Threat Categories: Confidentiality, Integrity, Availability; Wireless and Mobile Device Threats: Data Theft, System Access; Risk Mitigation and BYOD for SMBs; Security Standards and Regulatory Compliance (ISO, NIST, PCI DSS);

Module-3

WLAN Fundamentals and Threat Analysis:

How Do WLANs Work? WLAN Topologies, Service Sets, and Standards; Wireless Access Points (WAPs) and Antennas; Coverage Area Determination and Site Surveys; Spectrum and Protocol Analysis;

WLAN and IP Networking Threat and Vulnerability Analysis: Types of Attackers: Insiders vs. Outsiders; Physical Security, Social Engineering, and Wardriving; Rogue Access Points and Bluetooth Vulnerabilities; Malicious Data Insertion, Denial of Service, and Peer to Peer Hacking;

Module-4

Basic WLAN Security Measures: Design and Implementation for Security;

Authentication, MAC Filters, VPN, and VLANs; Wired Equivalent Privacy, WPA, WPA2; Ongoing Management Considerations (Firmware, Physical Security);

Advanced WLAN Security Measures: Comprehensive Security Policies; Authentication and Access Control (EAP, RADIUS); Intrusion Detection/Prevention Systems and Protocol Filtering; Advanced Data Protection: WPA2 Modes, VPN, IPsec; User Segmentation, VLANs, DMZ Segmentation; Device and Network Management;

Module-5

Advanced Mobile Security and Risk Management

WLAN Auditing Tools: Discovery Tools (NetStumbler, Kismet); Penetration Testing Tools (Metasploit, Aircrackng); Network Enumerators, Protocol Analyzers, and Attack Tools;

WLAN and IP Network Risk Assessment: Risk Assessment Methodologies and Stages; Security Risk Analysis and Audits; Legal Requirements and IT Security Management;

Mobile Communication Security Challenges: Mobile Phone Threats: Exploits, Tools, and Techniques; Security Architectures: Android, iOS, Windows Phone; BYOD and Enterprise Mobility Management;

Mobile Device Security Models: Security Models: Android, iOS, Windows Phone; Device Management, Encryption, and Handoff Challenges;

Textbooks:

J. Doherty, Wireless and Mobile Device Security. Jones & Bartlett Learning, 2nd edition Dec. 2021.

Reference Books

1. M. S. Obaidat, A. Anpalagan, I. Woungang, and S. Misra, *Security and Privacy in Wireless and Mobile Networks*. MDPI, 2021.
2. 2. M. Zinkus, T. M. Jois, and M. Green, "Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions," *arXiv*, 2021. [Online]. Available: https://arxiv.org/abs/2105.12613
3. J. Stevenson, Mobile Offensive Security Pocket Guide: A Quick Reference Guide for Android and iOS. Independently Published, 2022.

Course outcomes: The students should be able to:

- Explain the evolution and impact of wired and wireless networks.
- Identify and categorize security threats to wireless and mobile networks.
- Design and implement security measures for WLANs and mobile devices.
- Utilize security tools for auditing and penetration testing.
- Develop strategies to manage risks in mobile and wireless communication systems.

Internal Assessment Marks: 40 (3 Session Tests are conducted during the semester and Marks allotted based on average of all performances).

Subject Code:	BCY613D	TITLE: Wireless and Mobile Device Security		Faculty Name:	Ms.Sandhya G							
List of Course Outcomes	Program Outcomes											Total
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	
CO-1	2	2	-	-	2	-	-	-	-	-	-	2	8
CO-2	2	2	2	-	2	-	-	-	-	-	-	2	10
CO-3	2	2	2	-	2	-	-	-	-	-	-	3	11
CO-4	2	2	2	-	2	-	-	-	-	-	-	3	11
CO-5	2	2	-	-	2	-	-	-	-	-	-	3	9
Total	10	10	6	-	10	-	-	-	-	-	-	13	49

Note: 3 = Strong Contribution, 2 = Average Contribution, 1 = Weak Contribution, - = No Contribution

The Correlation of Course Outcomes (CO's) and Program Specific Outcomes (PSO's)

Subject Code:	BCY613D	TITLE: Wireless and Mobile Device Security	Faculty Name:	Ms. Sandhya G

List of Course Outcomes	Program Specific Outcomes		Total
	PSO-1	PSO-2	
CO-1	-	-	-
CO-2	-	-	-
CO-3	-	-	-
CO-4	-	-	-
Total	-	-	-