GUJARAT TECHNOLOGICAL UNIVERSITY

BRANCH: CYBER SECURITY (59)
SUBJECT NAME- MOBILE AND WIRELESS COMMUNICATION SECURITY
SUBJECT CODE- 2735901
SEMESTER-III

Type of course: Core

Prerequisite: Basics of Networking, Communications & Security

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
L	T	P	C	Theory Marks		Practical Marks				
				ESE (E)	PA (M)	PA (V)		PA(I)		
						ESE		PA	RP	
4	0	2	5	70	30	20	10	10	10	150

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	**UNIT – I Introduction to Wireless and Mobile Networks**		
	The Evolution of Data Networks: Data Networks, Internet, Computers, Mobile Phones, Convergence of Mobile & Data Networks, Basics of Network Security, Evolution of Cyber crime, Wireless network security, Mobile IP security	**02**	03
	Evolution of wired networking to wireless networking: OSI reference model, Economic impact of wireless networking, Wireless networking and the way people work, WiFi market & Developing nations, Internet of Things	**02**	03
	The Mobile Revolution: Mobile communication, evolution of mobile networks, Economic impact of mobile IP, Business impact of mobility, Business use cases	**02**	03
	Security Threats Overviews: Threat categories, Threats to wireless and Mobile devices, Risk mitigation, Authorization and Access control, Information security standards and regulatory compliance acts	**03**	04

2	**UNIT –II WLAN Security**		
	How do WLANs work? : WLAN topologies, 802.11 standards, Wireless Access Points, Wireless Bridges, Wireless Antennas	**02**	05
	WLAN and IP Networking and Threat and Vulnerability Analysis : Types of attackers, Targets, Physical security, Social engineering, Wardriving, Rogue Access Points, Bluetooth vulnerabilities and threats, Packet Analysis, Information theft, Malicious data insertion, Denial of Service attacks, Peer to Peer hacking over Ad hoc networks	**04**	08
	Basic WLAN Security Measures: Design and Implementation consideration for basic security, Authentication and Access Restriction, Data Protection, Ongoing Management Security Considerations	**03**	06
	Advanced WLAN Security Measures: Design & Implementation of Comprehensive Security Policy, Implementing Authentication and Access Control, Data Protection, User Segmentation, Managing Network and User Devices	**04**	08
	WLAN Auditing Tools:WLAN Discovery Tools, Penetration Testing Tools, Password Capture & Decryption Tools, Network Management & Control Tools, WLAN Hardware Audit Tools and Antennas, Attack Tools & Techniques, Network Utilities	**04**	08
	WLAN and IP Network Risk Assessment : Risk Assessment, IT Security Management, Security Risk Assessment Stages, Security Audits	**04**	08
3	**UNIT –III Mobile Security**		
	Mobile Communication Security Challenges: Mobile Phone Threats & Vulnerabilities, Exploits- Tools and Techniques, Google Android Security Challenges, Apple iOS Security Challenges, Windows Phone Security Challenges	**05**	10
	Mobile Device Security Models: Google Android Security, Apple iOS Security, Windows Phone Security, Security Challenges of Hand-Off type Features, BYOD and Security, Security using Enterprise Mobile Management	**05**	10
	Mobile Wireless Attacks and Mobile Remediation: Scanning the Corporate Network for Mobile Attacks, Client & Infrastructure Exploits, Network Security Protocol Exploits, Browser Application and Phishing Exploits, Mobile Software Exploits and Remediation	**05**	10
	Fingerprinting Mobile Devices: Types of fingerprinting, Fingerprinting Methods, Unique Device Identification, Software for Mobile Devices	**02**	04
	Mobile Malware and Application Based Threats: Malware on Android Devices, Malware on Apple iOS Devices, Malware on Windows Phone Devices, Mobile Malware Delivery Methods, Mobile Malware Defense, Mobile Device Management, Penetration Testing and Smartphones	**05**	10

Reference Books:

1. "Wireless and Mobile Device Security" Jim Doherty , Jones & Bartlett Learning
2. "Mobile and Wireless Design Essentials", MartynMallick, , Wiley Dreamtech India pvt ltd
3. "Mobile Communications", Jochen Schiller, Addision Wesley

Course Outcome:

After learning the course the students should be able to:

- **Understand security and threat aspects related to Mobile and Wireless Network.**
- **Assess risks in Wireless network and use auditing tools.**
- **Understand security models in Android, Apple and Windows phone and security challenges.**
- **Understand exploits and malware in Mobile phones**
- **Use tools for security of wireless network and mobile device to assess the risk and its remedy.**

List of Experiments:

Practical based on study and use of different tools mentioned in Unit –II and III.

Design based Problems (DP)/Open Ended Problem:

Case study based on real world scenario on Wireless Network to assess the risks and recommendation to minimize those risks.

Major Equipment:

Wireless Network setup, Mobile Devices, Laptop , Computers

List of Open Source Software/learning website:

1. **http://www.corecom.com/html/wlan_tools.html**
2. **http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf**
3. **https://www.cso.com.au/article/574311/mobile-security-ios-vs-android-vs-blackberry-vs-windows-phone/**
4. **https://arxiv.org/pdf/1505.07919.pdf**