GUJARAT TECHNOLOGICAL UNIVERSITY

COMPUTER ENGINEERING (SYSTEMS & NETWORK SECURITY) (56)
WIRELESS SECURITY
SUBJECT CODE: 2735601
M.E. 3rd SEMESTER

Type of course: Elective IV

Prerequisite: Information Security, Computer Networks

Rationale: Today when wireless systems are becoming popular, security in such network is a great concern. This Subject will help to understand how each of these different wireless technologies has different vulnerabilities and thus have different requirements for their 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)		
						PA	OEP	PA	RP	
3	2#	2	5	70	30	20	10	10	10	150

Content:

Sr. No	Topics	Teaching Hrs.	Module Weightage
1	Introduction to Wireless Network Security: Introduction, Protecting the Means Of Communication, Protecting Privacy, Promoting Safety, The Personal and the Public, Shaking Up the Status Quo, Understanding Wireless Forecasts, Reasonable Degrees of Security, Regulatory Environments and Issues, Security- Related Regulations, Security-Related Market Factors, Guidelines for Security Measures, Wireless Is Information Warfare (IW), Decision Theory, A Model for Cost-Effective Risk Management, Performance Measures and Key Design Tradeoffs, High-Level Performance Measures, Low-Level Performance Measures, Military- Unique System Requirements, Offensive Information Operations, Cryptographic Attacks, Defensive Information Operations, Cryptographic Measures, Key Management, Electromagnetic Capture Threats.	6	15
2	Telephone System Vulnerabilities: Interception/Ease of Interception, Interruption of Service, Unintentional Interruptions, Natural Hazards, Intentional Interruptions, Cell Phone Vulnerabilities	4	10
3	The Wireless Local Area Network (WLAN) Wireless Transmission Media, Securing WLANs, Securing WLANs, The Infamous WEP, Physical Security	4	15
4	Wireless Application Protocol(WAP) Comparison of the TCP/IP, OSI, and WAP Models, WAP Security	4	10

	Architecture, Marginal Security		
5	Wireless Transport Layer Security (WTLS) Secure Socket Layer, Wireless Transport Layer Security and WAP	3	10
6	Bluetooth Introduction To Bluetooth, Security Functions at the Baseband Layer, Security Functions of the Service Discovery Protocol, Security Functions at the Link Layer, Frequency-Hopping, Channel Establishment, Security Manager, Authentication, Authentication with the SAFER1 Block Cipher, Encryption, Encryption Modes, Key Length Negotiation, Encryption With the E0 Stream Cipher, Threats to Bluetooth Security, Jamming, Bluetooth holes	6	15
7	Upcoming Wireless Networks: MANET and WSN: Introduction, upcoming wireless networks: Wireless mesh network, Hybrid Ad hoc Network, Mobile Ad hoc Network, Vehicular Networks, Sensor Networks, RFID, Mobility in Internet, Trends and security challenges in wireless network, Routing Protocols in MANET, Attacks on Ad hoc networking protocols, Securing ad hoc network routing protocols, Provable security for ad hoc network routing protocols, Secure routing in sensor network, Key Management in WSNs.	4	10%

Reference Books:

1. Wireless Security-Models, Threats, and Solutions By Randall K. Nichols, Panos C. Lekkas (McGrawHill)
2. Security and Cooperation in Wireless Networks, by Buttyan and Hubaux
3. Research papers and web Resources

Course Outcome:

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

1. To recognize the threats and vulnerabilities unique to wireless networks
2. To learn things from the point of view of the manager and policy maker, the designer and the project lead

List of Experiments:

1. Implement Flooding Attack in MANET.
2. Implement Selfish node attack in MANET
3. Implement Black hole attack in MANET.
4. Implement Gray hole attack in MANET.
5. Implement various Key Management protocols in WSN.
6. Case Study: Wireless Transport Layer security Implementations

Design based Problems (DP)/Open Ended Problem:

1. Study of performance of MANET on various parameters such as PDR, End to End Delay, Overhead, Energy Efficiency in which each of the attack mentioned in Experiments has been implemented.
2. Study of performance of various Routing Protocols of MANET/WSN with regards to security parameters.
3. Study of changes to be made in the existing protocols to mitigate against various security attacks

Major Equipments: Latest PC with required software

List of Open Source Software/learning website:NS-2

Review Presentation (RP): The concerned faculty member shall provide the list of peer reviewed Journals and Tier-I and Tier-II Conferences relating to the subject (or relating to the area of thesis for seminar) to the students in the beginning of the semester. The same list will be uploaded on GTU website during the first two weeks of the start of the semester. Every student or a group of students shall critically study 2 papers, integrate the details and make presentation in the last two weeks of the semester. The GTU marks entry portal will allow entry of marks only after uploading of the best 3 presentations. A unique id number will be generated only after uploading the presentations. Thereafter the entry of marks will be allowed. The best 3 presentations of each college will be uploaded on GTU website.