Gujarat Technological University

GTU Cyber Security Research Group

(Networks of Researchers at GTU)

Report of Workshop on

1. WEB APPLICATION VULNERABILITIES

By: Dr. DEEPAK SINGH TOMAR
Department of Computer Science & Engineering
M.A. National Institute of Technology, Bhopal

2. SECURITY ISSUES IN WIRELESS NETWORKS

By: Dr. Vrinda Tokekar
Professor & Head, Department of Information Technology
Institute of Engineering & Technology
Devi Ahilya Vishwavidyalaya, Indore

Organized by

GTU PG Research Center for Cyber Security

Date: 27st March-2015

POST-GRADUATE RESEARCH CENTRES: -Gujarat Technological University has set up 14 Postgraduate Research Centres to foster research activities. The GTU Post-graduate Research Centre for Cyber Security is one of the 14 research centres.

The Post-graduate Research Centres work as catalysts for infusing the spirit of innovation and research among the GTU community, through actively involving Faculty Members of Engineering, Architecture, Planning and Management and post-graduate students in research and development. The Centres are supposed to encourage Faculty Members and research students to apply for research grants and establish research laboratories. The Centres are to establish active linkages with the industry and research institutions in India and abroad.

The Centres also aim to become institutional 'public intellectuals' or independent think-tanks to which scholars of the whole world should be invited and where they would like to come to expound their ideas to a receptive, knowledgeable but critical audience.

CYBERSECURITY RESEARCH GROUP: GTU has established the Cybersecurity Research Group for creating a network of researchers and Faculty Members, working in the area of cybersecurity in all the Colleges, so that they can jointly inter-act with the rest of the world, grow themselves and develop the profile of their respective Departments and Colleges.

The Research Groups are associated with the Research Centers. Every Group is designed to involve researchers and Faculty Members in all the Colleges in research in a hub-and-spoke model, with the Center working as the coordinating hub. GTU provides all the necessary infrastructural support in addition to organizing Seminars, Workshops and Expert Lectures, in the areas of interest to the Research Groups.

During GTU Research Week 2015, more than 100 workshops are being organized at GTU which are being recorded / broadcast live to achieve greater reach. As a part of this ou-reach program, GTU PG Center for Cyber Security recently organized two workshops on Cybersecurity where **more than 200 research scholars actively participated physically at GTU Chandkheda campus and through live broadcast on internet at three GTU affiliated colleges.**

The objective of the workshop was to create awareness about the recent substantial increase of research & development, adoption in cyber security work and considerable amount of contributions to this domain from India in various areas like vulnerability, security policy, localization, critical information infrastructure.

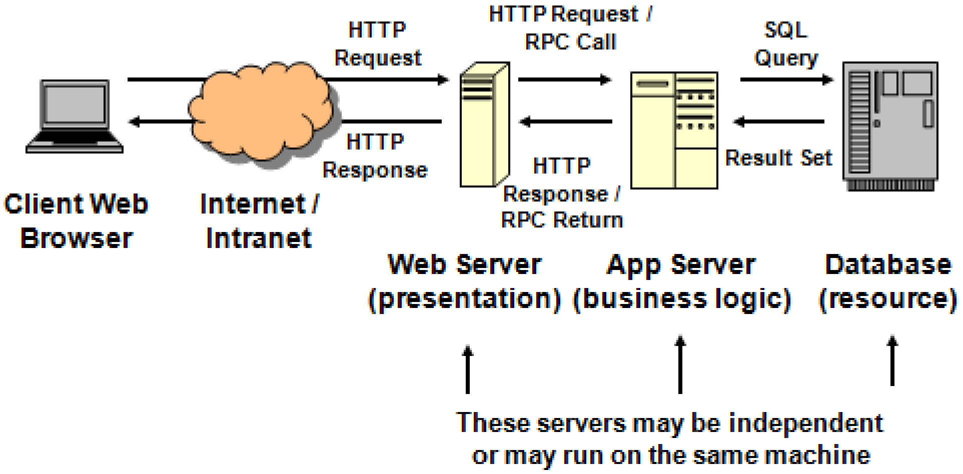
The primary focus of this workshop was to share knowledge about issues in wireless network and Challenges and in Web application vulnerability.

The workshop commenced at 3:00 P.M by Dr. Deepak Singh Tomar and his presentation was on Web Application Vulnerability.

Technical Session by Dr. Deepak Singh Tomar from 03:00 PM to 04:00 PM:

Dr Tomar covered the following areas during his talk:

- threats and attacks on networks
- vulnerabilities
- Three tier web application architecture as follow


HTTP Request
HTTP Response
HTTP Request / RPC Call
HTTP Response / RPC Return
SQL Query
Result Set
Client Web Browser
Internet / Intranet
Web Server (presentation)
App Server (business logic)
Database (resource)
These servers may be independent or may run on the same machine

- Common type of code injection attack and practical demo of it.
  1. SQL injection
  2. Cross Side Scripting
  3. PHP Code injection

- **Open Web Application Security Project (OWASP)**: The Open Web Application Security Project (OWASP) is an open community and nonprofit organization which is dedicated to finding and fighting the causes of insecure software. It provides a powerful awareness document for web application security. In every three years it releases and ranks the top 10 vulnerabilities

- **Packet Sniffing**: *Packet sniffing* is the monitoring of data traffic into and out of a computer or network. In some networks, data transmissions are sent only to the machine they are intended for, while in others, transmissions are broadcast to all machines connected, but processed only by the target computer. In the latter cases, it is possible to packet-sniff a computer using only another computer on the same network, without placing any software or equipment on the surveyed machine.

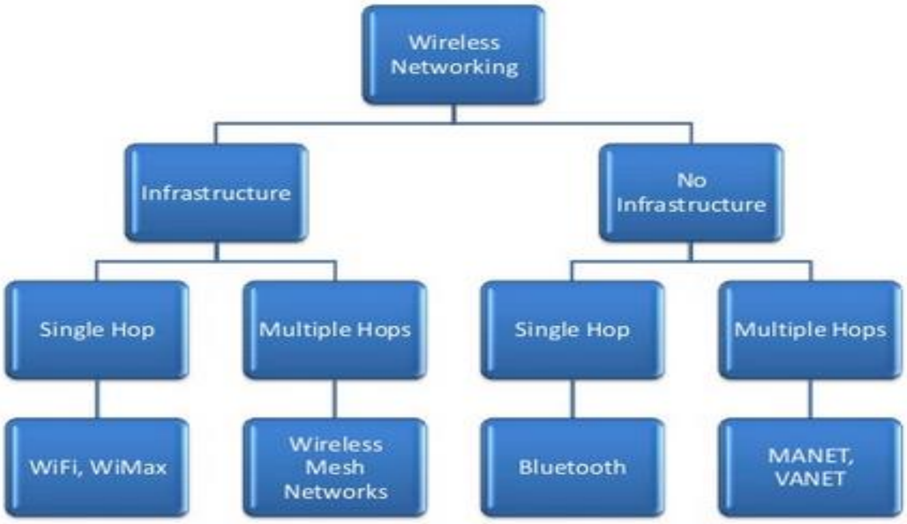
- **Phishing Attack**: The act of sending an email that falsely claims to be from a bank or other E-commerce enterprise. To trick the recipient into surrendering private information that will be used for identity theft. The information is usually about usernames/passwords; credit card, social security, and bank account numbers

- **Banner Grabbing**: Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running on open ports. Banner grabbing is an attack designed to deduce the brand and/or version of an operating system or application.

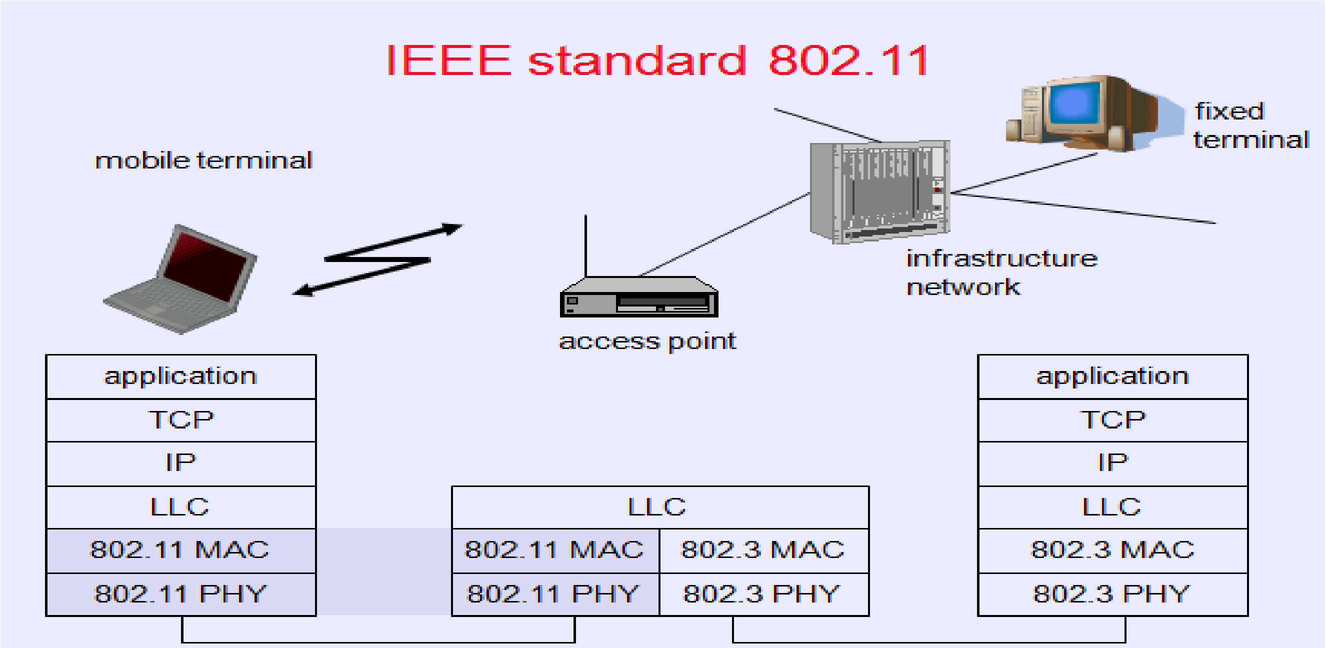
Technical Session by Dr. Vrinda Tokekar from 04:15 PM to 05:00 PM :

Dr Takekar covered the following areas during her talk:

- **Taxonomy of Wireless Networks & its Characteristics as below:**



- **Description of Cellular Systems and its components**
- **WiFi - Wireless LANs and its standards**



IEEE standard 802.11

mobile terminal
application
TCP
IP
LLC
802.11 MAC
802.11 PHY

access point	
LLC	
802.11 MAC	802.3 MAC
802.11 PHY	802.3 PHY

fixed terminal
application
TCP
IP
LLC
802.3 MAC
802.3 PHY

Challenges in Mobile Environments

1. Limitations of the Wireless Network
   - Packet loss due to transmission errors
   - Variable capacity links
   - Frequent disconnections/partitions
   - Limited communication bandwidth
2. Limitations Imposed by Mobility
   - dynamically changing topologies/routes
   - lack of mobility awareness by system/applications
3. Limitations of the Mobile Computer
   - short battery lifetime
   - limited capacities

- **Wireless Vulnerabilities and security issues as follows:**
  1. Detectability
     - Users do not want their wireless systems to be detected e.g. soldiers in military field
     - Signal should not be detected
  2. Resource Depletion/exhaustion
     - Resources (computing, bandwidth) are limited
     - Depletion attack : shortens battery life
     - Exhaustion attack : consumes battery power
  3. War driving/walking/chalking
     - Techniques to Search for open wireless network and to know their unprotected status
     - War Driving : Taking computer with wireless card and detection software and moving through some vehicle to search wireless network

- ➢ War Walking: Taking lightweight computer and walking through area to search wireless network
- ➢ War Chalking : Marking presence and status of wireless network as open, closed or WEP protected

4. Pre-keying: Key Management problem, key creation, storing, distribution
5. Reconfiguring: Ad hoc networks have dynamic topology, Nodes move in/out of network, Security components must provide more protection than simply leaving nodes and network "wide open"
6. Hostile Environment : Physical boundary does not exist – eavesdropping becomes easier

- **Approaches to Security of Wireless Networks:**

1. Limit the Signal by Wire integrity and tapping & Physical Limitation
2. Encryption by Public and Private key encryption: leads to computational and data overhead
3. Integrity Codes :
   - Checksum versus Cryptographic Hash
   - Message Authentication code
   - Payload versus Header
4. Traffic Analysis
   - Provide key exchange protocol, message integrity, and encapsulation
   - IPSec
5. Authentication Protocols
   - Point to Point Protocol (PPP)
   - Challenge Handshake Authentication Protocol (CHAP)
   - Extensible Authentication Protocol (EAP)

There are many research ideas shared by the expert in the field of wireless communication. Students interacted a lot and asked lots of questions to the expert.

Researchers, who wants to join this Research Group may contact:
Mr. Darshan Patel (Asst. Prof) (ap_darshan@gtu.edu.in)
Ms. Kinjal Dave (Asst. Prof) (kjdave-itsns@gtu.edu.in)
Mr. Bhadreshsinh Gohil (Asst. Prof) (bhadresh-wimc@gtu.edu.in)
Mr. Vagmin Joshi (Asst. Prof) (ap_vagmin@gtu.edu.in)

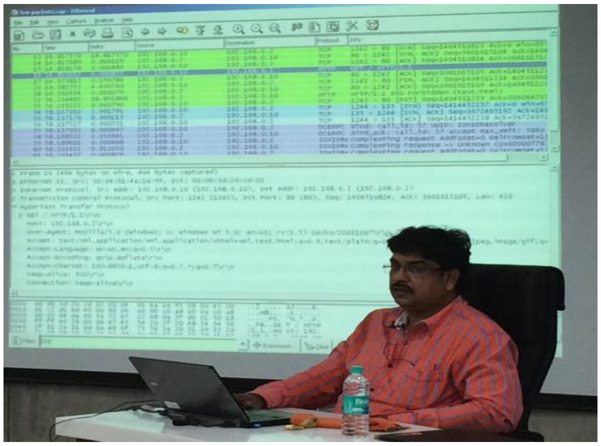
Report prepared by: Darshan Patel

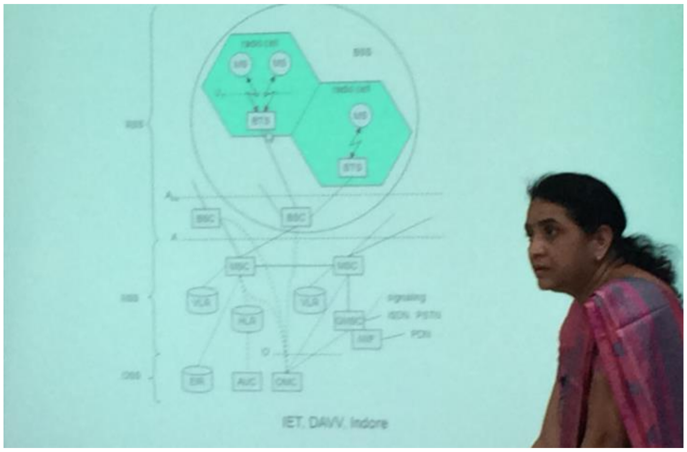
Reference: For a report of the Advisory Board of e-Raksha Research Center meeting of 27th January 2015, please see http://www.gtu.ac.in/circulars/15Jan/Report_e-Raksha_Adviory_Meeting_27-Jan-2015_2.pdf

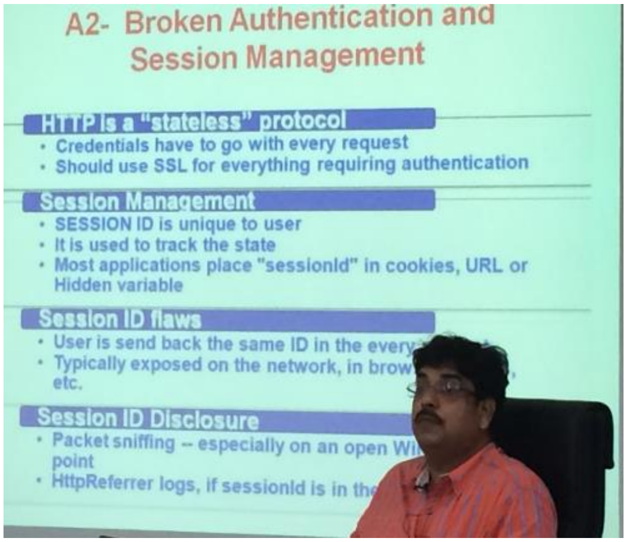
Report of the previous meeting of the Research Group on 23rd January 2015 is available at http://www.gtu.ac.in/circulars/15Mar/16032015.pdf

Report of the Workshop on Cryptography of 6th February 2015 at http://www.gtu.ac.in/circulars/15feb/12022015_01.pdf

WORKSHOP PHOTO GALLERY







A2- Broken Authentication and Session Management

HTTP is a "stateless" protocol

- Credentials have to go with every request
- Should use SSL for everything requiring authentication

Session Management

- SESSION ID is unique to user
- It is used to track the state
- Most applications place "sessionId" in cookies, URL or Hidden variable

Session ID flaws

- User is send back the same ID in the every
- Typically exposed on the network, in brow , etc.

Session ID Disclosure

- Packet sniffing -- especially on an open Wi point
- HttpReferrer logs, if sessionId is in the