CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

INSTITUTE : UIE

DEPARTMENT : CSE

Bachelor of Engineering (Computer Science & Engineering)

WEB AND MOBILE SECURITY (Professional Elective-I)

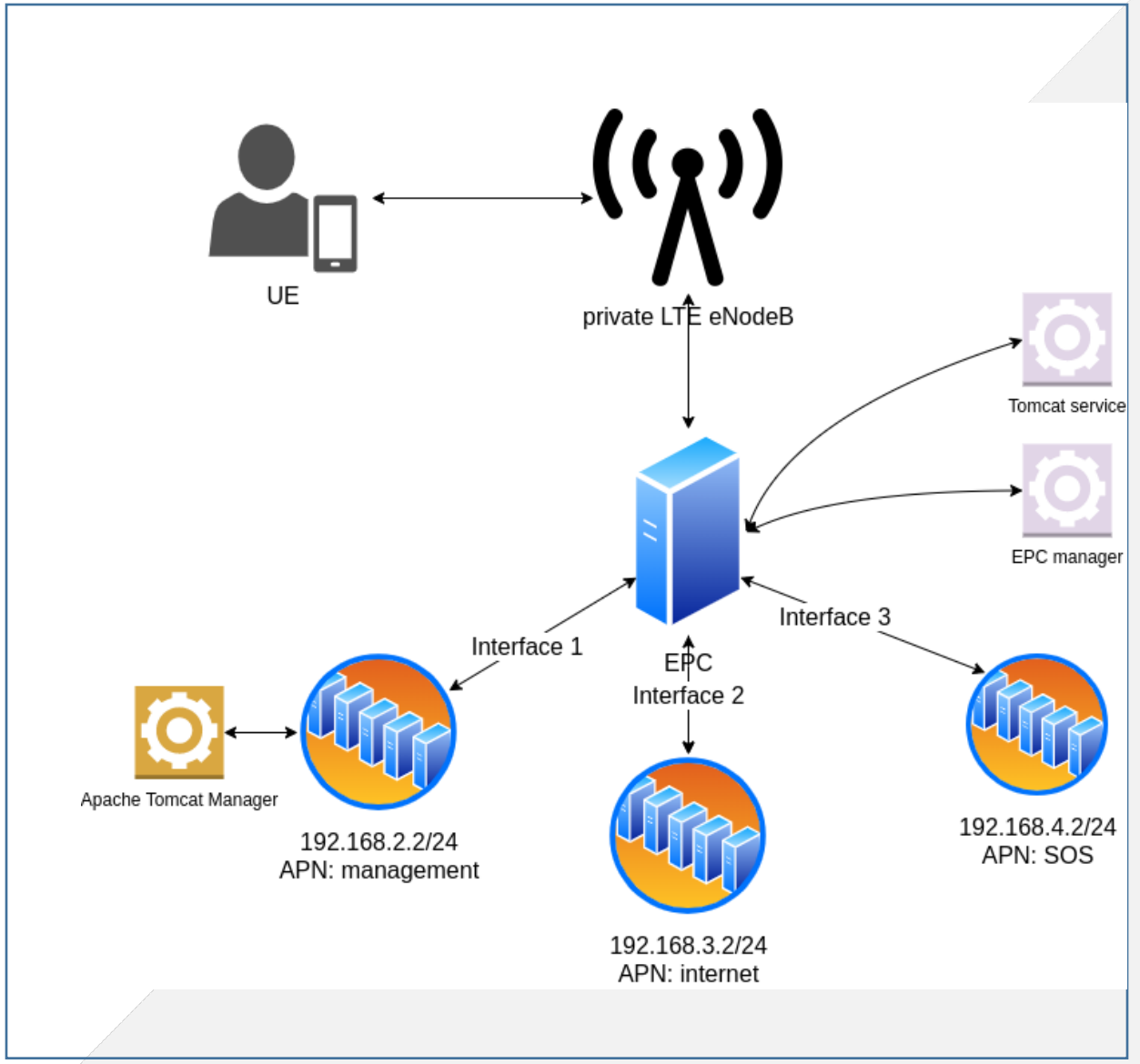
(20CST/IT-333)

TOPIC OF PRESENTATION:

Wi-Fi and Bluetooth Security

Lecture Objectives

In this lecture, we will discuss:
Bluetooth Security, Wi-Fi Security



Wi-Fi Security: WEP vs WPA or WPA2

- WEP, WPA, and WPA2 are Wi-Fi security protocols that secure wireless connections. They keep your data hidden and protect your communications, while blocking hackers from your network. Generally, WPA2 is the best choice, even though it consumes more processing power to protect your network. Learn more about Wi-Fi security options and how encryption tools like VPNs can protect you even further.

Wi-Fi Security

- All Wi-Fi security protocols are certified by the **Wi-Fi Alliance**, the non-profit organization that owns the Wi-Fi trademark. There are four wireless security protocols currently available:
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA 2)
- Wi-Fi Protected Access 3 (WPA 3)

What are some ways to protect a Wi-Fi network?

- One basic best practice for Wi-Fi security is to change default passwords for network devices.
- Most devices feature default administrator passwords, which are meant to make setup of the devices easy. However, the default passwords created by device manufacturers can be easy to obtain online.
- Changing the default passwords for network devices to more-complex passwords—and changing them often—are simple but effective ways to improve Wi-Fi security. Following are other Wi-Fi network security methods:

- A more common method of protecting Wi-Fi networks and devices is the use of security protocols that utilize encryption. Encryption in digital communications encodes data and then decodes it only for authorized recipients.
- There are several types of encryption standards in use today, including Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). See the section "Types of wireless security protocols" on this page for more details about these and other standards related to Wi-Fi security.

- PNs are another source of Wi-Fi network security. They allow users to create secure, identity-protected tunnels between unprotected Wi-Fi networks and the internet.
- A VPN can encrypt a user's internet connection. It also can conceal a user's IP address by using a virtual IP address it assigns to the user's traffic as it passes through the VPN server.

What is Bluetooth security ?

- Bluetooth security is of paramount importance as devices are susceptible to a variety of wireless and networking attacking including denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation.
- Bluetooth security must also address more specific Bluetooth related attacks that target known vulnerabilities in Bluetooth implementations and specifications. These may include attacks against improperly secured Bluetooth implementations which can provide attackers with unauthorized access.

There are three basic means of providing Bluetooth security

- ***Authentication:*** In this process the identity of the communicating devices are verified. User authentication is not part of the main Bluetooth security elements of the specification.
- ***Confidentiality:*** This process prevents information being eavesdropped by ensuring that only authorised devices can access and view the data.
- ***Authorisation:*** This process prevents access by ensuring that a device is authorised to use a service before enabling it to do so.

Security issues

- ***Bluejacking:*** Bluejacking is often not a major malicious security problem, although there can be issues with it, especially as it enables someone to get their data onto another person's phone, etc. Bluejacking involves the sending of a vCard message via Bluetooth to other Bluetooth users within the locality - typically 10 metres. The aim is that the recipient will not realise what the message is and allow it into their address book. Thereafter messages might be automatically opened because they have come from a supposedly known contact
- ***Bluebugging:*** This more of an issue. This form of Bluetooth security issue allows hackers to remotely access a phone and use its features. This may include placing calls and sending text messages while the owner does not realise that the phone has been taken over
- ***Car Whispering:*** This involves the use of software that allows hackers to send and receive audio to and from a Bluetooth enabled car stereo system
- In order to protect against these and other forms of vulnerability, the manufacturers of Bluetooth enabled devices are upgrading he security to ensure that these Bluetooth security lapses do not arise with their products.

References:

Books:

1. Hacking Exposed Mobile: Security Secrets & Solutions 1st Edition, Kindle Edition, by Neil Bergman, Mike Stanfield, Jason Rouse, and Joel Scambray
2. Hacking Exposed Web Applications, 3rd edition, Joel Scambray, Vincent Liu, Caleb Sima, Released October 2010, Publisher(s): McGraw-Hill

Reference Links:

https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php
https://www.actcorp.in/blog/wep-wpa-wpa2-wifi-security

Relevant Videos:

https://www.youtube.com/watch?v=WqBR6jd0IbU
https://www.youtube.com/watch?v=LLq1WnY1GjQ

THANK YOU