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)

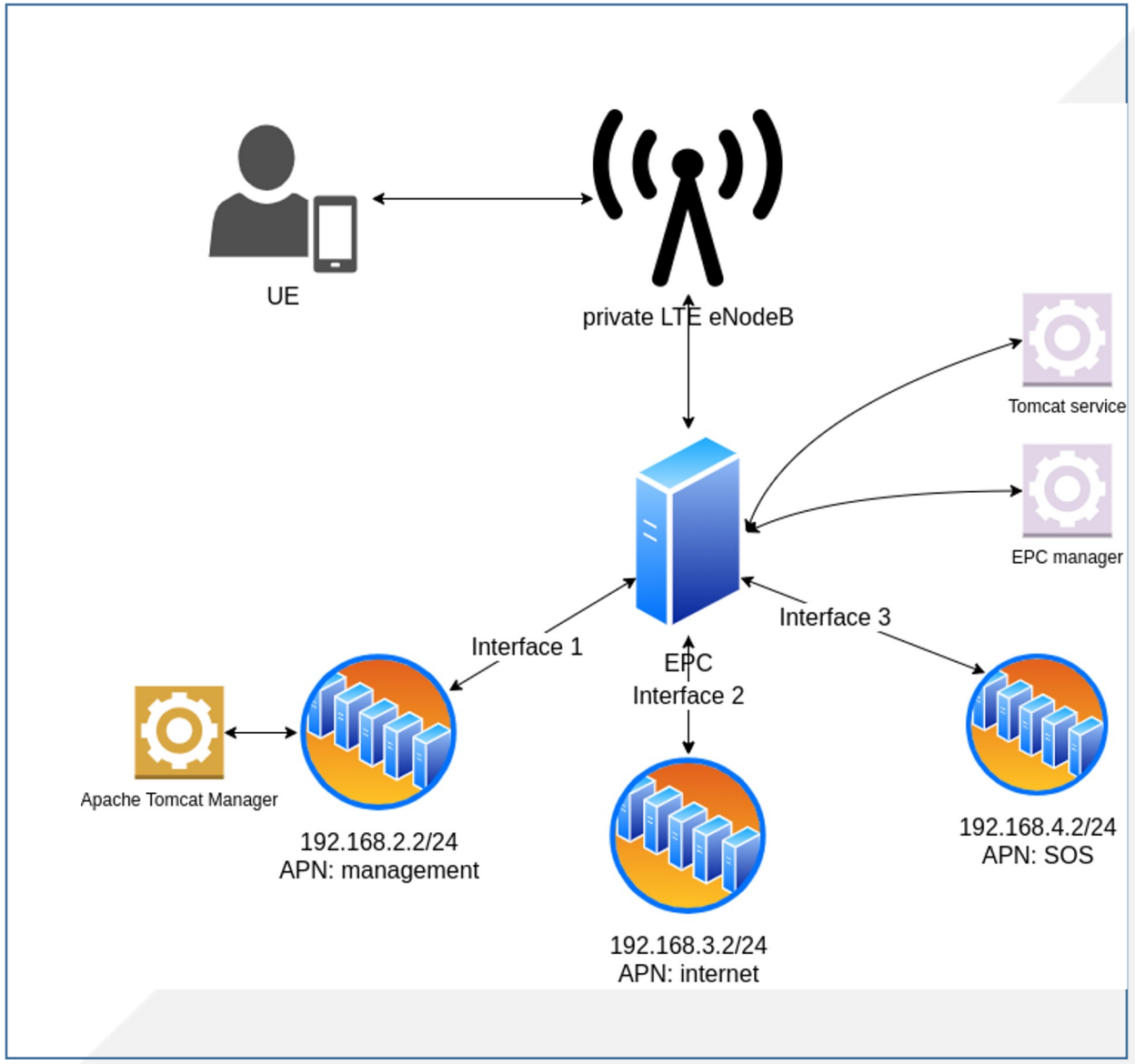
TOPIC OF PRESENTATION:

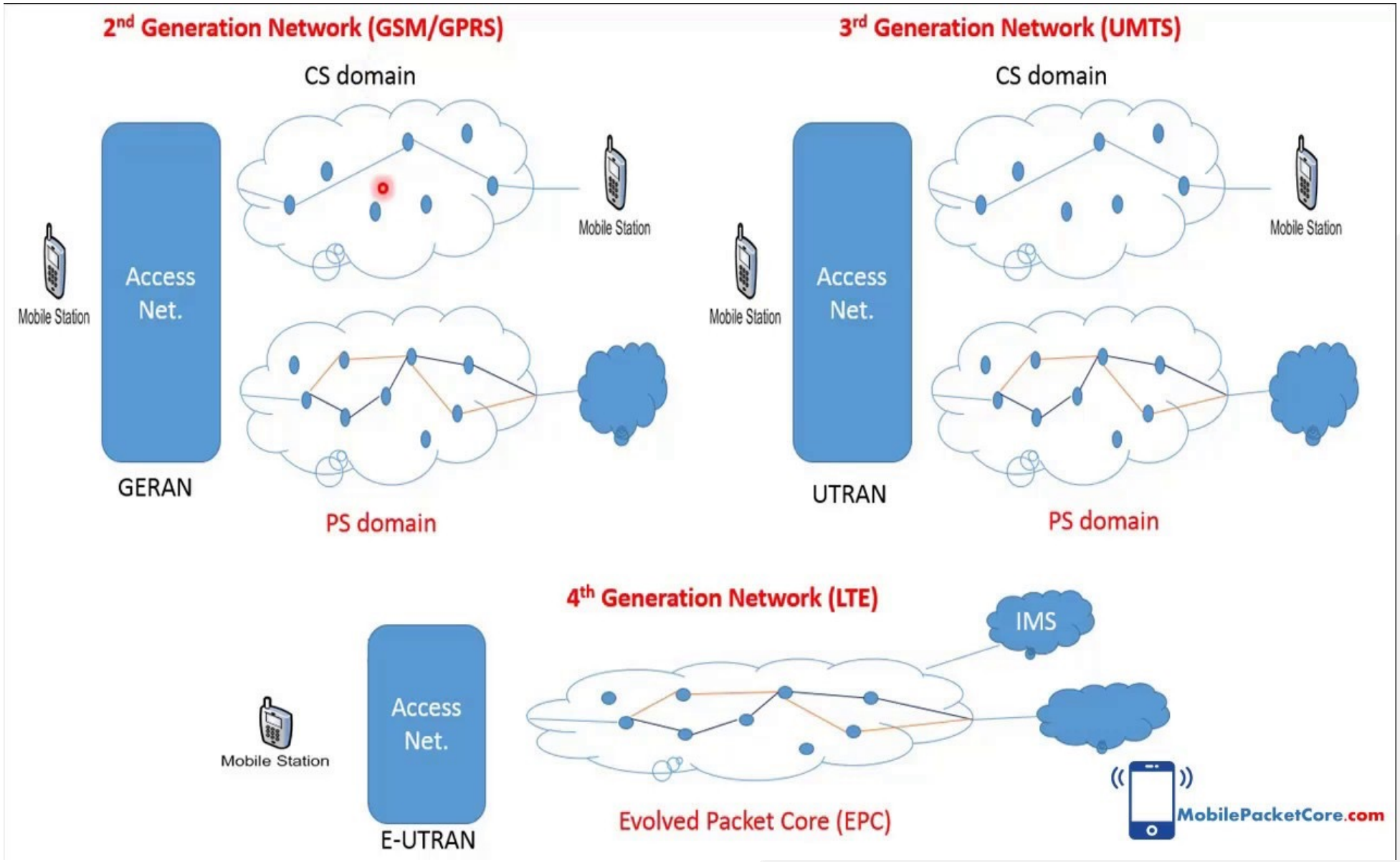
Mobile Security-Security of GSM Networks, Security of UMTS Networks

DISCOVER . LEARN . EMPOWER

Lecture Objectives

In this lecture, we will discuss:
Mobile Security-Security of GSM Networks, Security of UMTS and LTE Networks




2nd Generation Network (GSM/GPRS)
CS domain
Mobile Station
Access Net.
Mobile Station
GERAN
PS domain
3rd Generation Network (UMTS)
CS domain
Mobile Station
Access Net.
Mobile Station
UTRAN
PS domain
4th Generation Network (LTE)
IMS
Mobile Station
Access Net.
E-UTRAN
Evolved Packet Core (EPC)
MobilePacketCore.com

Difference Between GSM, UMTS And LTE?

GSM	UMTS	LTE
Second-generation (2G) cellular technology	Third-generation (3G) cellular technology	Fourth-generation (4G) cellular technology
Digital network	Digital network	Digital network
Other 2G technologies: D-AMPS, IS-95	Other 3G technologies: CDMA2000	Other 4G technologies: WiMAX (but LTE is the primary 4G technology)
Radio access: FDMA and TDMA	Radio access: Wideband CDMA (WCDMA)	Radio access: OFDMA and SC-FDMA
1991-92	2000	2009
Circuit-Switched & Packet-Switched	Circuit-Switched & Packet-Switched	Packet-Switched
Enhancements: GPRS and EDGE	Enhancements: HSPA and HSPA+	Enhancements: LTE-Advanced & LTE Advanced Pro
Peak data rate: 384 kbps with EDGE	Peak data rate: 42 Mbps with HSPA+	Peak data rate: 3 Gbps with LTE-Advanced Pro
Channel bandwidth: 200 kHz	Channel bandwidth: 5 MHz mainly but 10 MHz and 20 MHz are also possible	Channel bandwidth: 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz and 20 MHz

https://commsbrief.com/difference-between-gsm-umts-lte/

GSM

The GSM network is divided in 4 sections :

- Mobile Stations The subscriber will use a mobile station to make and receive calls via the GSM network. The MS is composed of two distinct functional entities, the subscriber identity module (SIM), which is a removable smart card, and the mobile equipment.
- Base Station Subsystem (BSS) The MS communicates with the base transceiver station (BTS) via the radio interference. A BTS performs all the transmission and reception functions relating to the GSM.
- Network Management Every BSS is connected to a Mobile services switching centre (MSC). The MSC is concerned with the routing of calls to and from the mobile users. The Home Location Center (HLR) is used to store information that is specific to each subscriber. Every GSM subscriber will have a record in the HLR.

Security features

- The subscriber is uniquely identified by the International Mobile Subscriber Identity (IMSI). This information, along with the individual subscriber authentication key (Ki), constitutes sensitive identification credentials analogous to the Electronic Serial Number (ESN) in analog systems such as AMPS and TACS. Security in GSM consists of the following aspects:
- • Authentication
- • Signal and Data confidentiality
- • Identity confidentiality

Algorithms

- Encryption algorithms GSM algorithms were developed in secret, official descriptions were not published to the public. Most of the information available come from leaked documents and cryptanalysis projects. GSM specifications define 3 algorithms:
- A3 the authentication algorithm.
- A8 the key generation algorithm.
- A5 the encryption algorithm.

https://web.itu.edu.tr/~korkusuza/Security%20in%20the%20GSM%20Network.pdf?kategori=php

UMTS network

UMTS is designed to interoperate with GSM networks. To protect GSM networks against man-in-middle attacks, 3GPP is considering to add a structure RAND authentication challenge.

- Five security groups exist in UMTS networks as shown in the figure.
  - Network Access Security
  - Network domain security
  - User domain security
  - Application domain security
  - visibility, configurability of security

https://www.rfwireless-world.com/Tutorials/3G-security.html

UMTS Security

- The security functions of UMTS are based on what was implemented in GSM. Some of the security functions have been added and some existing have been improved. Encryption algorithm is stronger and included in base station (NODE-B) to radio network controller (RNC) interface , the application of authentication algorithms is stricter and subscriber confidentially is tighter. The main security elements that are from GSM:
- Authentication of subscribers
- Subscriber identity confidentially
- Subscriber Identity Module (SIM) to be removable from terminal hardware
- Radio interface encryption

Additional UMTS security features:

- Security against using false base stations with mutual authentication
- Encryption extended from air interface only to include Node-B to RNC connection
- Security data in the network will be protected in data storages and while transmitting ciphering keys and authentication data in the system.
- Mechanism for upgrading security features.

https://www.umtsworld.com/technology/security.htm

LTE security

LTE authentication is the process of determining whether a user is an authorized subscriber to the network that he/she is trying to access, while NAS security and AS security are **features required to securely deliver user data that travels through LTE radio links at NAS and AS levels**.

Voice over LTE (VoLTE) is a packet-based telephony service seamlessly integrated into the Long Term Evolution (LTE) standard. By now all major telecommunication operators use VoLTE. **To secure the phone calls, VoLTE encrypts the voice data between the phone and the network with a stream cipher**.

Integrity

"0000" EIA0 Null Integrity Protection algorithm

"0001" 128-EIA1 SNOW 3G

"0010" 128-EIA2 AES

Ciphering

"0000" EEA0 Null ciphering algorithm

"0001" 128-EEA1 SNOW 3G based algorithm

"0010" 128-EEA2 AES based algorithm

https://www.3glteinfo.com/lte-security-architecture/

https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf

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.cse.iitb.ac.in/~vishalprajapati08/Study/CS649/GSM%20and%20UMTS%20Security%20Report.pdf

https://www.tutorialspoint.com/umts/umts_authentication.htm

https://www.geeksforgeeks.org/difference-between-umts-and-gsm/

https://www.umtsworld.com/technology/security.htm

Relevant Videos:

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

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

THANK YOU