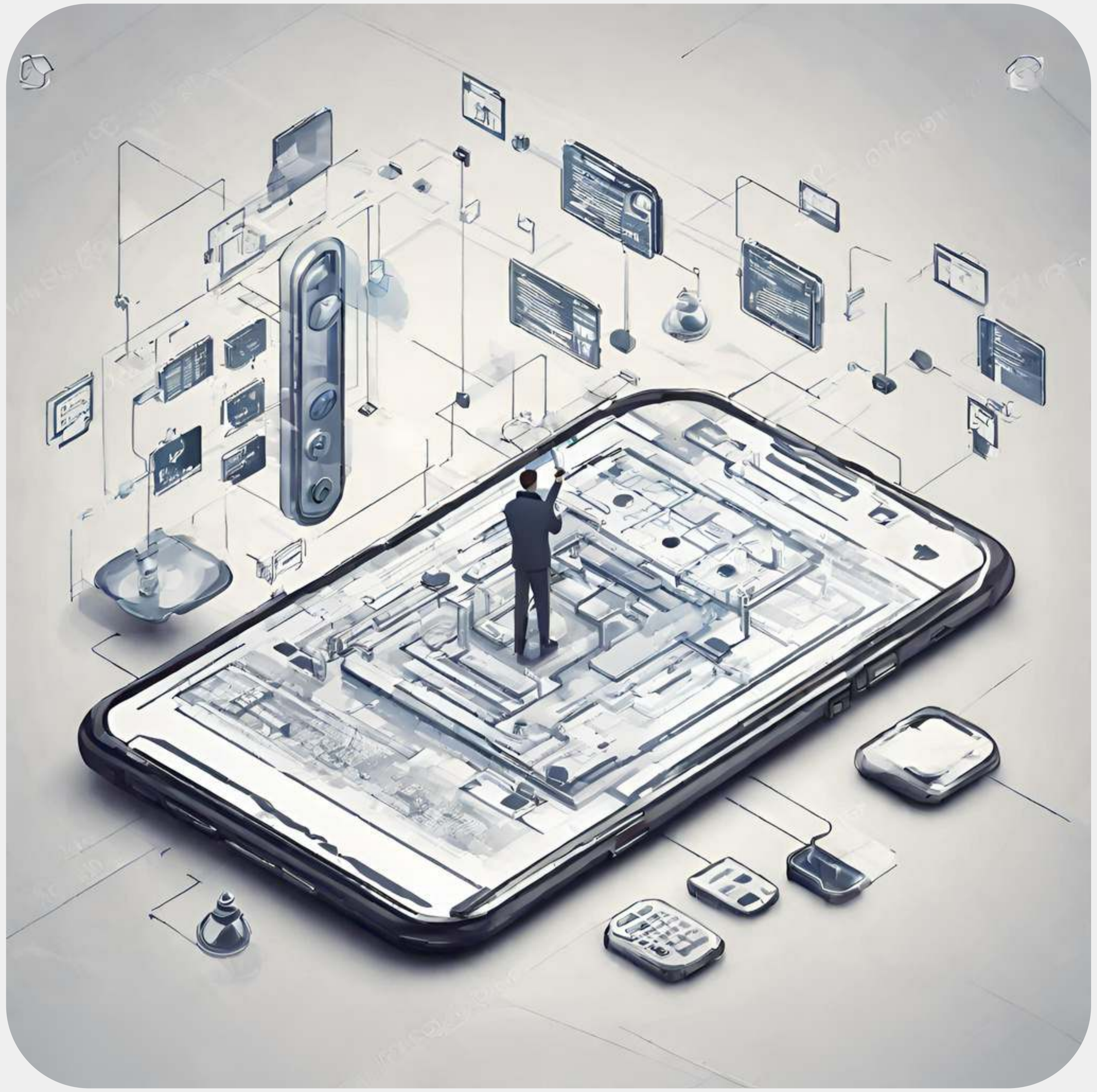
BAKI ALİ NEFT MƏKTƏBİ
BAKU HIGHER OIL SCHOOL

Mobile development and security

Session 14



Karim Karimov

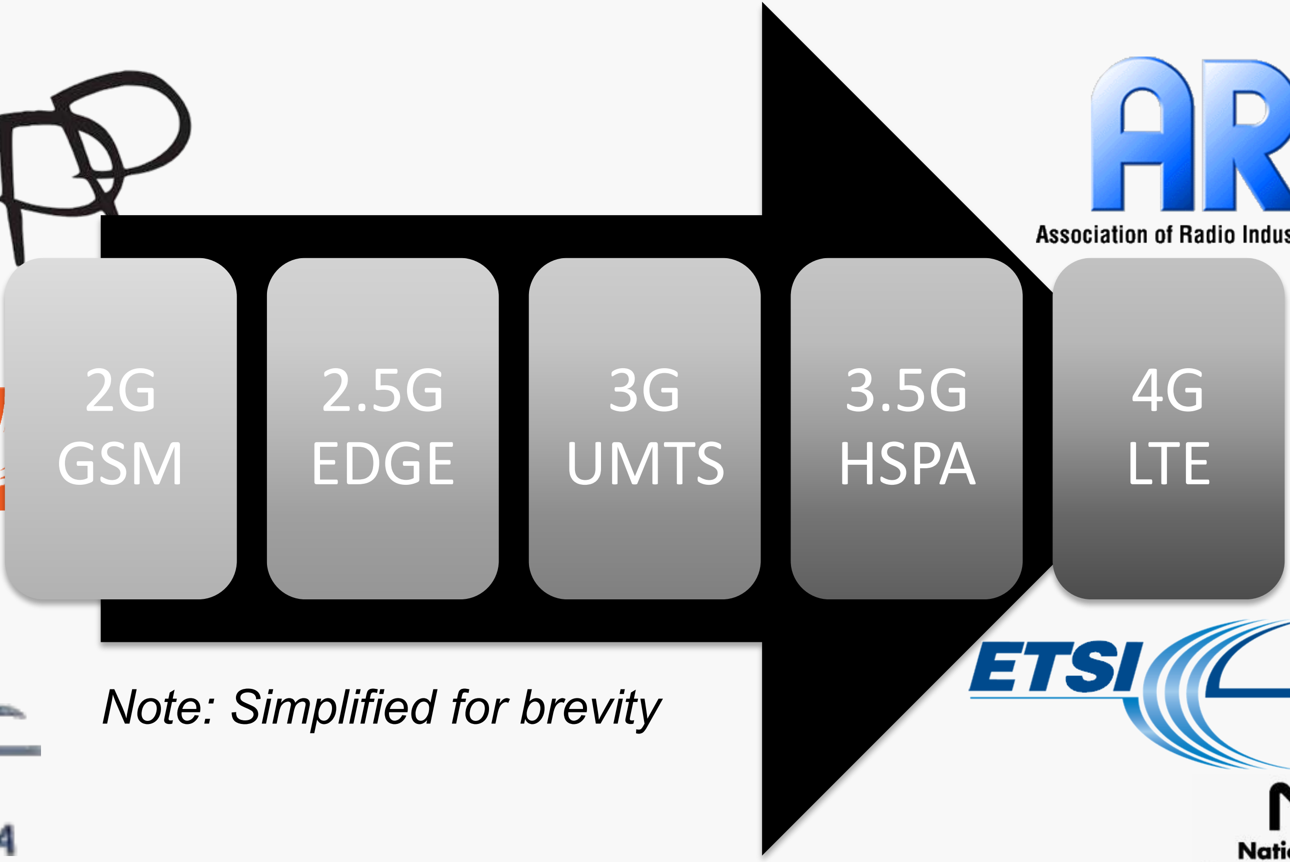
Lecturer

3GPP Standards & Evolution

3GPP

atis

CCSA



2G
GSM

2.5G
EDGE

3G
UMTS

3.5G
HSPA

4G
LTE

Note: Simplified for brevity

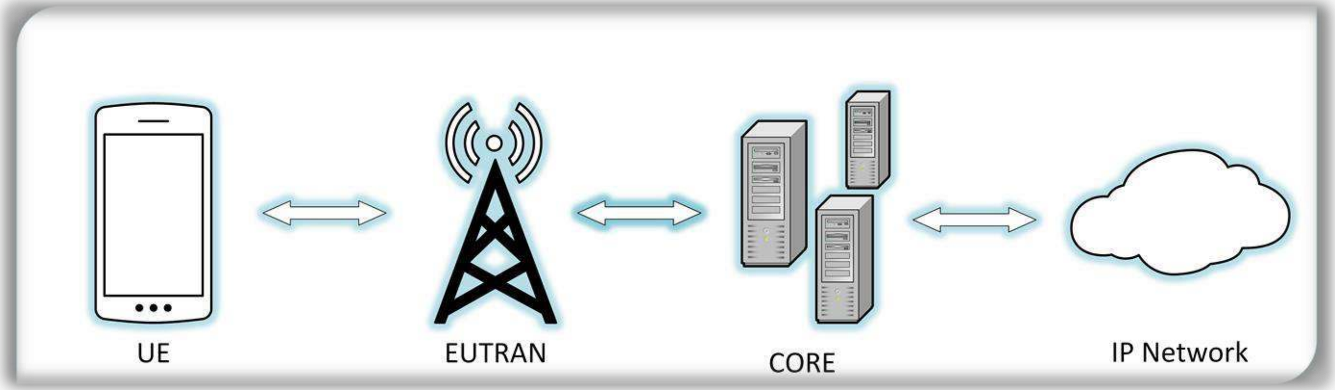
ARIB
Association of Radio Industries and Businesses

ETSI

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The Basics

- A device (UE) connects to a network of base stations (E-UTRAN)
- The E-UTRAN connects to a core network (Core)
- The Core connects to the internet (IP network).

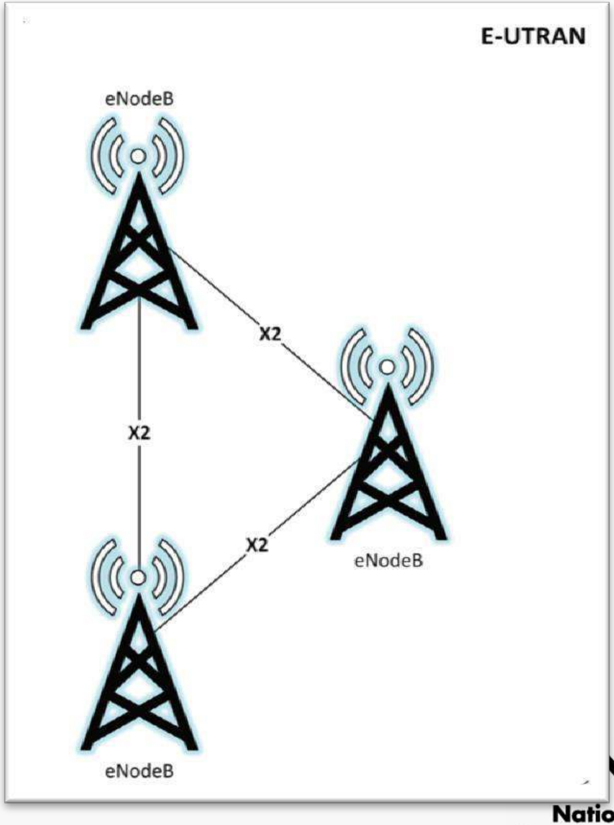


Mobile Device

- **User equipment (UE):** Cellular device containing the following
  - **Mobile equipment (ME):** The physical cellular device
  - **UICC:** Known as SIM card
    - Responsible for running the SIM and USIM Applications
    - Can store personal info (e.g., contacts) & even play video games!
  - **IMEI:** Equipment Identifier
  - **IMSI:** Subscriber Identifier

The Evolved Universal Terrestrial Radio Access Network (E-UTRAN)

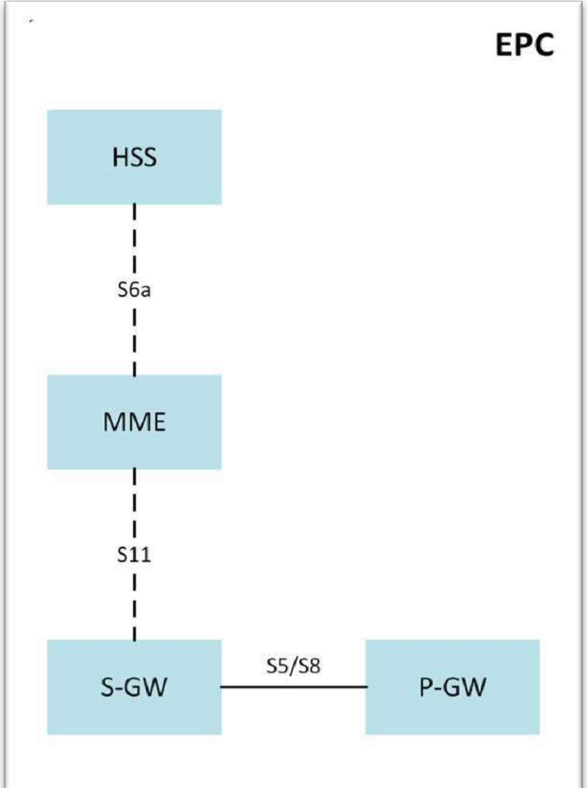
- **eNodeB:** Radio component of LTE network
  - De-modulates RF signals & transmits IP packets to core network
  - Modulates IP packets & transmits RF signals to UE
- **E-UTRAN:** mesh network of eNodeBs
- **X2 Interface:** connection between eNodeBs



National Institute of Standards and Technology
U.S. Department of Commerce

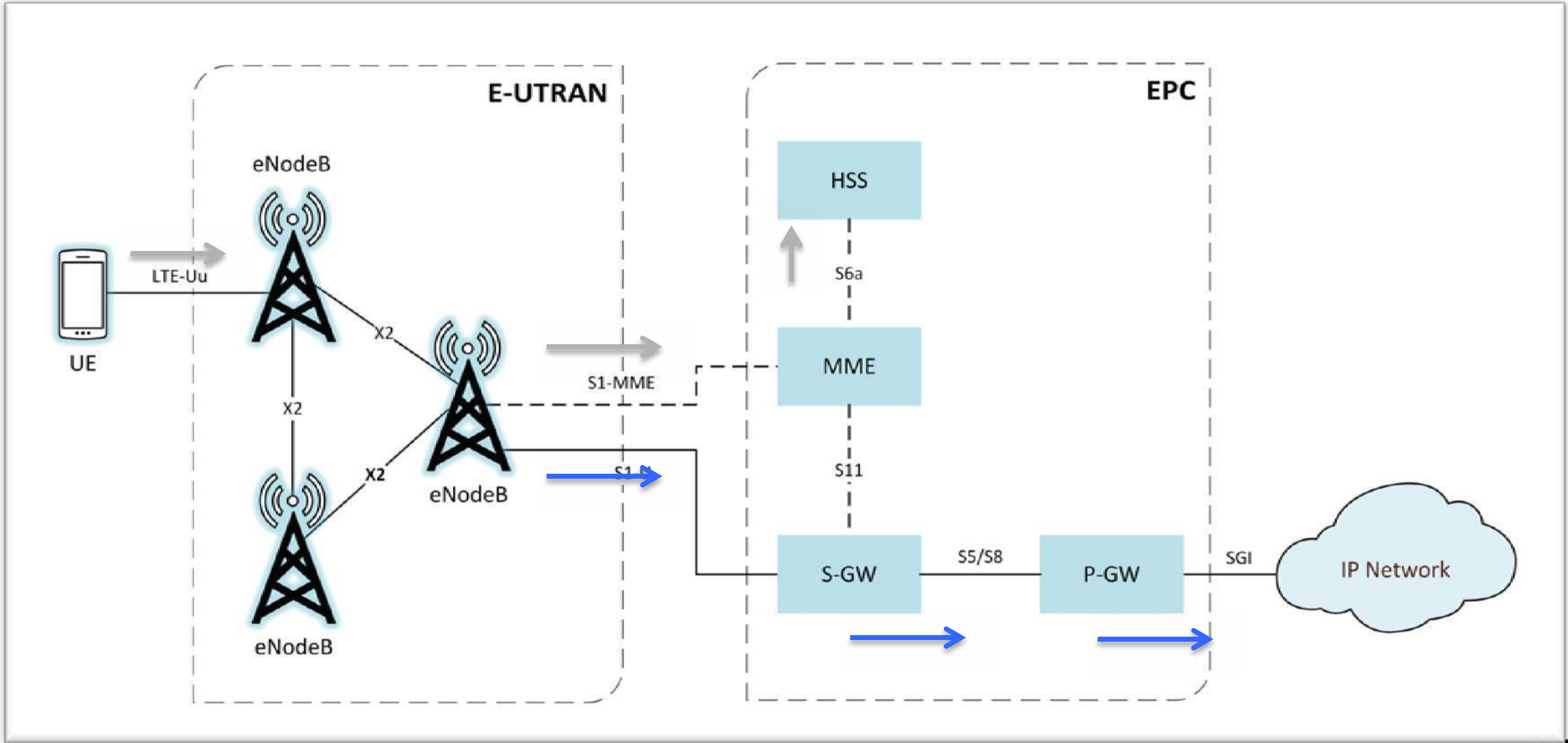
Evolved Packet Core (EPC)

- **Mobility Management Entity (MME)**
  - Primary signaling node - does not interact with user traffic
  - Functions include managing & storing UE contexts, creating temporary IDs, sending pages, controlling authentication functions, & selecting the S-GW and P-GWs
- **Serving Gateway (S-GW)**
  - Router of information between the P-GW and the E-UTRAN
  - Carries user plane data, anchors UEs for intra-eNodeB handoffs
- **Packet Data Gateway (P-GW)**
  - Allocates IP addresses and routes packets
  - Interconnects with non 3GPP networks
- **Home Subscriber Server (HSS)**
  - Houses subscriber identifiers and critical security information



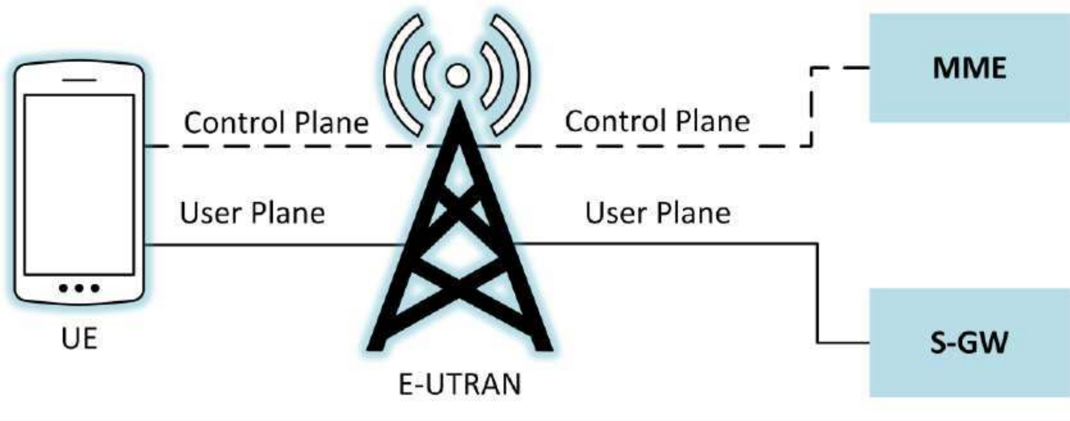
Note: Simplified for brevity

LTE Network


E-UTRAN
EPC
eNodeB
UE
LTE-Uu
X2
X2
X2
eNodeB
eNodeB
S1-MME
S1-U
HSS
S6a
MME
S11
S-GW
S5/S8
P-GW
SGI
IP Network

Communications Planes

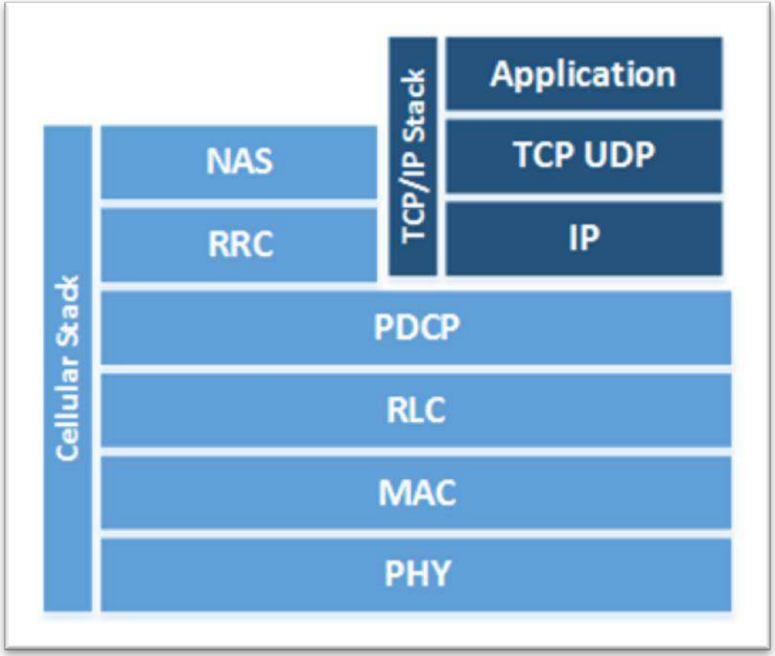
- LTE uses multiple planes of communication
- Different logical planes are multiplexed into same RF signal
- Routed to different end points



LTE Protocols

TCP/IP sits on top of the cellular protocol stack:

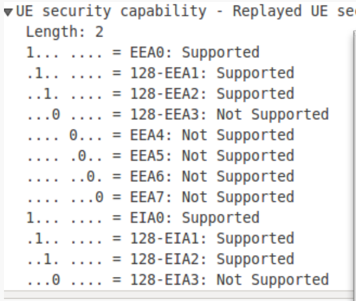
- **Radio Resource Control (RRC):** Transfers NAS messages, AS information may be included, signaling, and ECM
- **Packet Data Convergence Protocol (PDCP):** header compression, radio encryption
- **Radio Link Control (RLC):** Readies packets to be transferred over the air interface
- **Medium Access Control (MAC):** Multiplexing, QoS



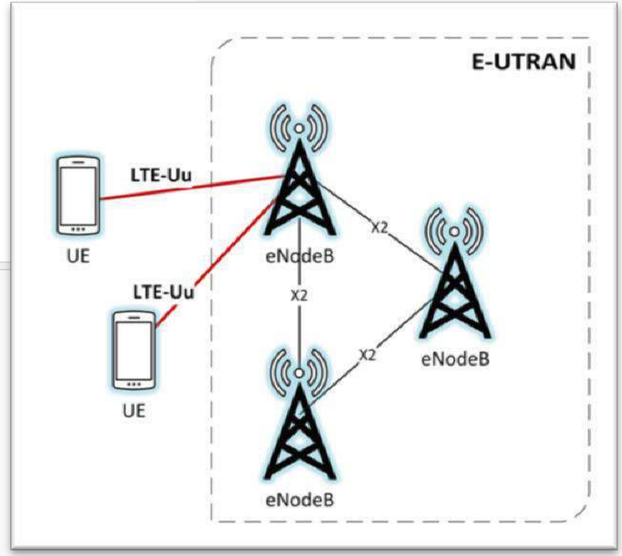
LTE Security Architecture

Air Interface Protection

- The connection between the UE and the eNodeB is referred to as the air interface
- 3 algorithms exist to protect the LTE air interface:
  - SNOW 3G = stream cipher designed by Lund University (Sweden)
  - AES = Block cipher standardized by NIST (USA)
  - ZUC = stream cipher designed by the Chinese Academy of Sciences (China)
- Each algorithm can be used for confidentiality protection, integrity protection, or to protect both.



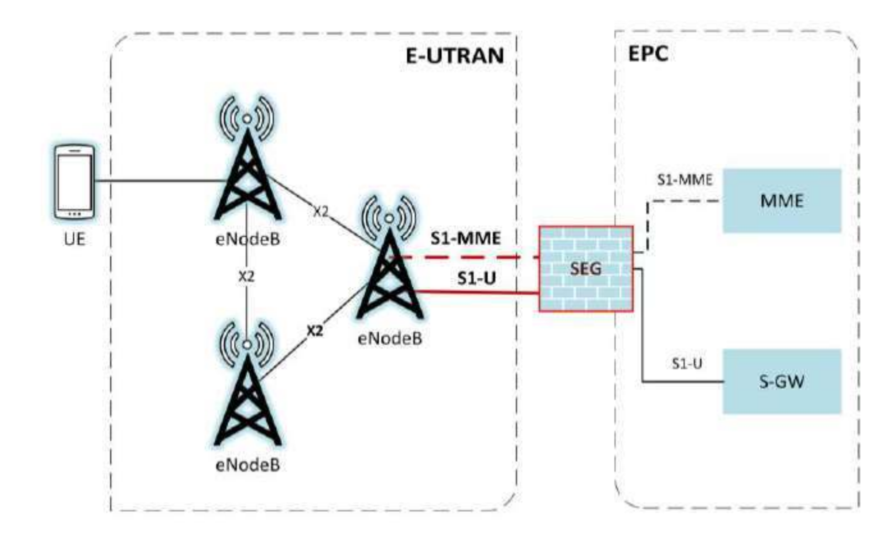
```
▼UE security capability - Replayed UE security capabilities
   Length: 2
   1... .... = EEA0: Supported
   .1.. .... = 128-EEA1: Supported
   ..1. .... = 128-EEA2: Supported
   ...0 .... = 128-EEA3: Not Supported
   .... 0... = EEA4: Not Supported
   .... .0.. = EEA5: Not Supported
   .... ..0. = EEA6: Not Supported
   .... ...0 = EEA7: Not Supported
   1... .... = EIA0: Supported
   .1.. .... = 128-EIA1: Supported
   ..1. .... = 128-EIA2: Supported
   ...0 .... = 128-EIA3: Not Supported
```



3GPP 33.401- 5.1.3.1: User plane confidentiality protection shall be done at PDCP layer and is an operator option.

Backhaul Protection

- Confidentiality protection of traffic running over S1 Interface (Backhaul)
- Hardware security appliances are used to implement this standard
- Security Gateways (SEG)
- IPSEC tunnel created between eNodeB and SEG



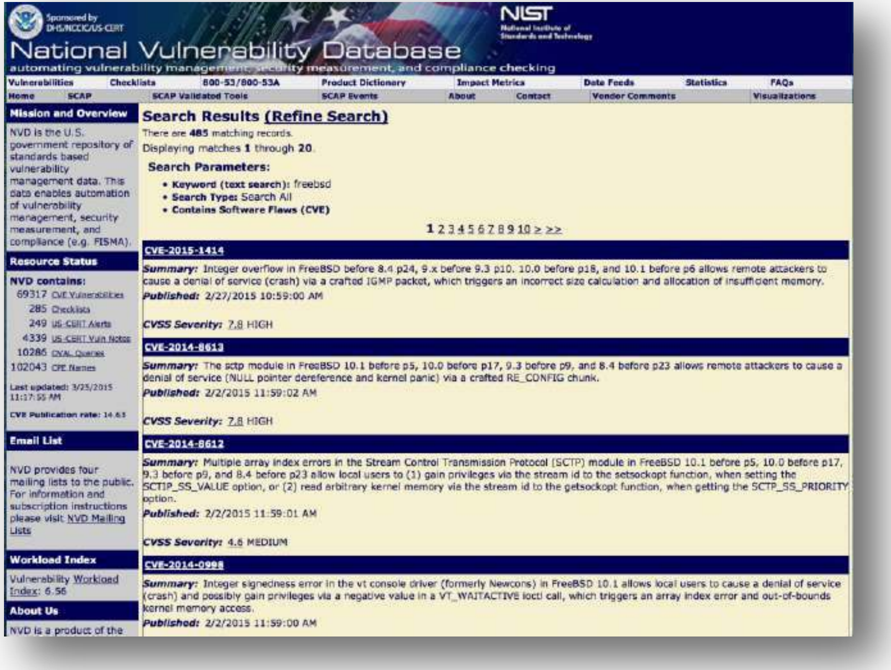
3GPP TS 33.401 - 13: NOTE: In case the S1 management plane interfaces are trusted (e.g. physically protected), the use of protection based on IPsec/IKEv2 or equivalent mechanisms is not needed.

Threats to LTE Networks

National Institute of
Standards and Technology
U.S. Department of Commerce

General Computer Security Threats

- **Threat:** LTE infrastructure runs off of commodity hardware & software.
  - With great commodity, comes great responsibility.
  - Susceptible to software and hardware flaws pervasive in any general purpose operating system or application
- **Mitigation:** Security engineering and a secure system development lifecycle.


Sponsored by DHS/NCCIC/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
800-53/800-53A
Product Dictionary
Impact Metrics
Data Feeds
Statistics
FAQs
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments
Visualizations

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

69317	CVE Vulnerabilities
285	Checklists
249	US-CERT Alerts
4339	US-CERT Vuln Notes
10286	OVAL Queries
102043	CPE Names

Last updated: 3/25/2015 11:17:55 AM

CVE Publication rate: 14.63

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Workload Index

Vulnerability Workload Index: 6.56

About Us

NVD is a product of the

Search Results (Refine Search)

There are **485** matching records.
Displaying matches **1** through **20**.

Search Parameters:

- **Keyword (text search):** freebsd
- **Search Type:** Search All
- **Contains Software Flaws (CVE)**

1 2 3 4 5 6 7 8 9 10 > >>

CVE-2015-1414

Summary: Integer overflow in FreeBSD before 8.4 p24, 9.x before 9.3 p10. 10.0 before p18, and 10.1 before p6 allows remote attackers to cause a denial of service (crash) via a crafted IGMP packet, which triggers an incorrect size calculation and allocation of insufficient memory.

Published: 2/27/2015 10:59:00 AM

CVSS Severity: 7.8 HIGH

CVE-2014-8613

Summary: The sctp module in FreeBSD 10.1 before p5, 10.0 before p17, 9.3 before p9, and 8.4 before p23 allows remote attackers to cause a denial of service (NULL pointer dereference and kernel panic) via a crafted RE_CONFIG chunk.

Published: 2/2/2015 11:59:02 AM

CVSS Severity: 7.8 HIGH

CVE-2014-8612

Summary: Multiple array index errors in the Stream Control Transmission Protocol (SCTP) module in FreeBSD 10.1 before p5, 10.0 before p17, 9.3 before p9, and 8.4 before p23 allow local users to (1) gain privileges via the stream id to the setsockopt function, when setting the SCTIP_SS_VALUE option, or (2) read arbitrary kernel memory via the stream id to the getsockopt function, when getting the SCTP_SS_PRIORITY option.

Published: 2/2/2015 11:59:01 AM

CVSS Severity: 4.6 MEDIUM

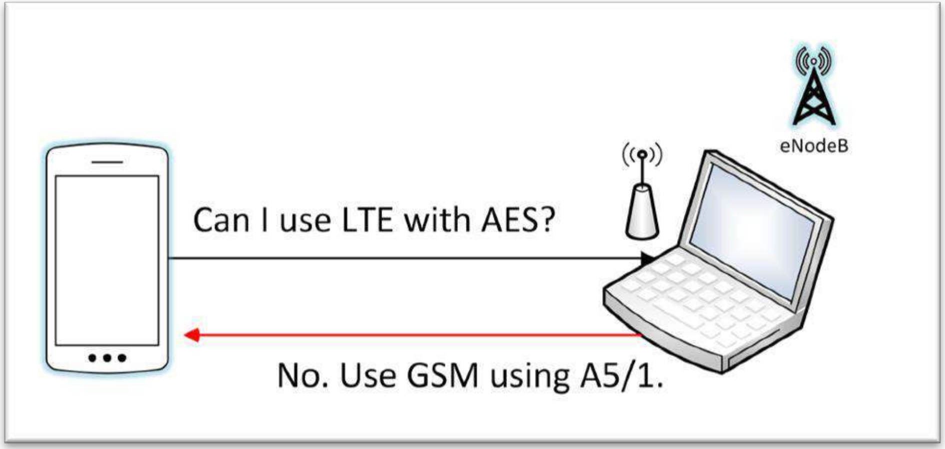
CVE-2014-0998

Summary: Integer signedness error in the vt console driver (formerly Newcons) in FreeBSD 10.1 allows local users to cause a denial of service (crash) and possibly gain privileges via a negative value in a VT_WAITACTIVE ioctl call, which triggers an array index error and out-of-bounds kernel memory access.

Published: 2/2/2015 11:59:00 AM

Renegotiation Attacks

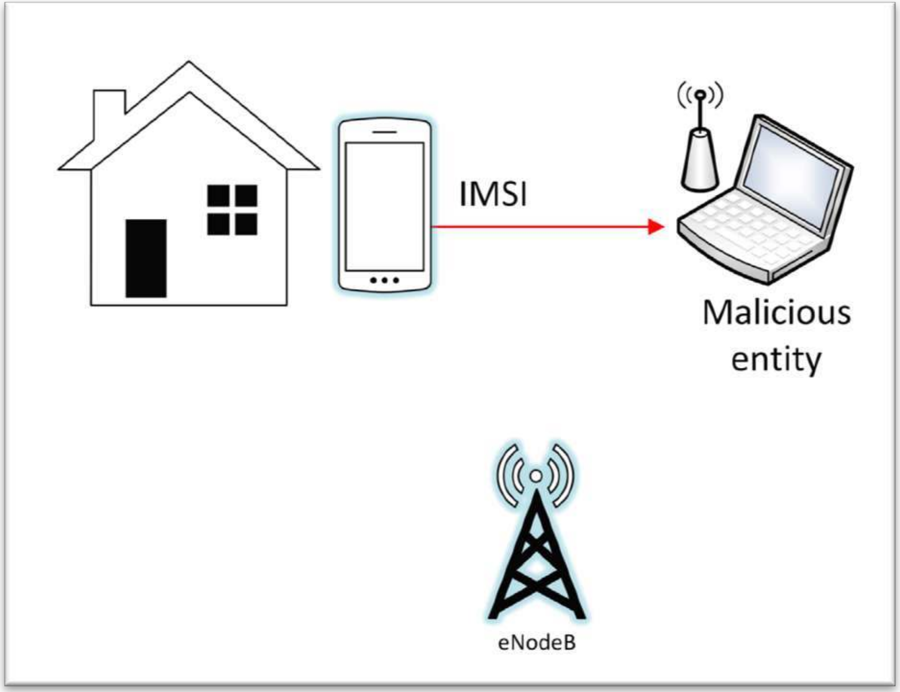
- **Threat:** Rogue base stations can force a user to downgrade to GSM or UMTS.
  - Significant weaknesses exist in GSM cryptographic algorithms.
- **Mitigation:**
  - Ensure LTE network connection. Most current mobile devices do not provide the ability to ensure a user's mobile device is connected to an LTE network.
  - A ‘Use LTE only’ option is available to the user
  - Use a rogue base station detector



National Institute of Standards and Technology
U.S. Department of Commerce

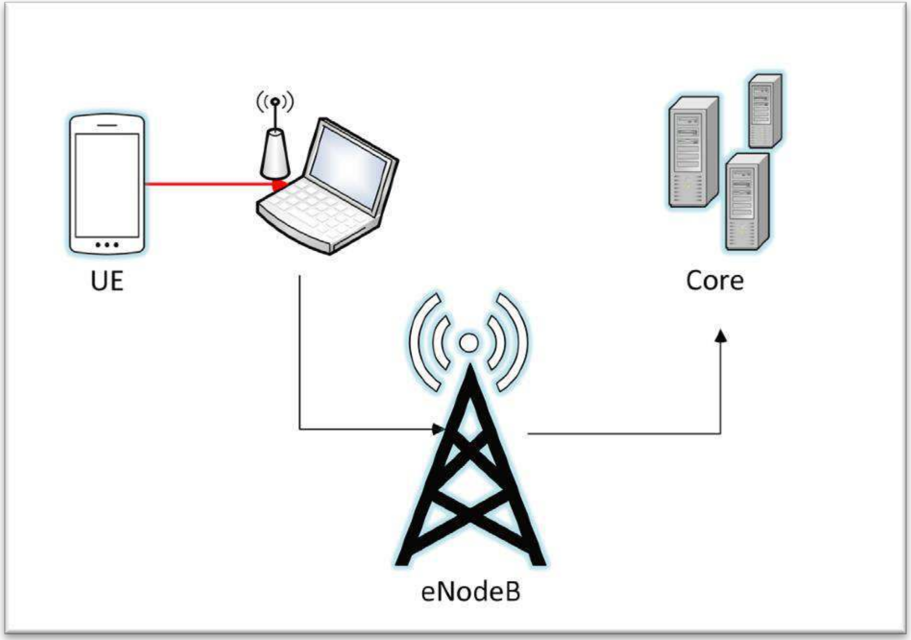
Device & Identity Tracking

- **Threat:** The IMEI and IMSI can be intercepted and used to track a phone and/or user.
  - Rogue base stations can perform a MiM attack by forcing UEs to connect to it by transmitting at a high power level
  - The phone may transmit its IMEI or IMSI while attaching or authenticating.
- **Mitigation:**
  - UEs should use temporary identities and not transmit them in over unencrypted connections.
  - IMSI-catcher-catcher



Call Interception

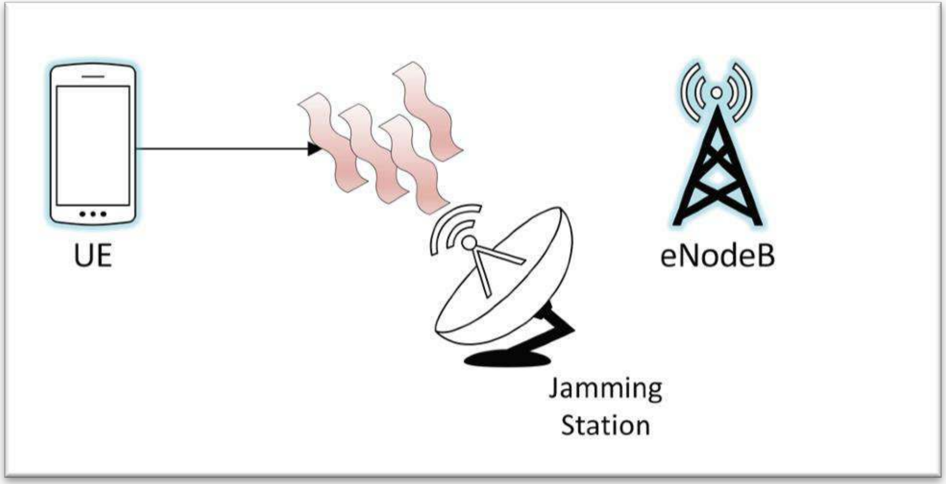
- **Threat:** Renegotiation attacks may also allow MitM attacks to establish an unencrypted connection to a device making a phone call
  - Attacker may be able to listen to the phone call
- **Mitigation:** The ciphering indicator feature discussed in 3GPP TS 22.101 would alert the user if calls are made over an unencrypted connection



National Institute of Standards and Technology
U.S. Department of Commerce

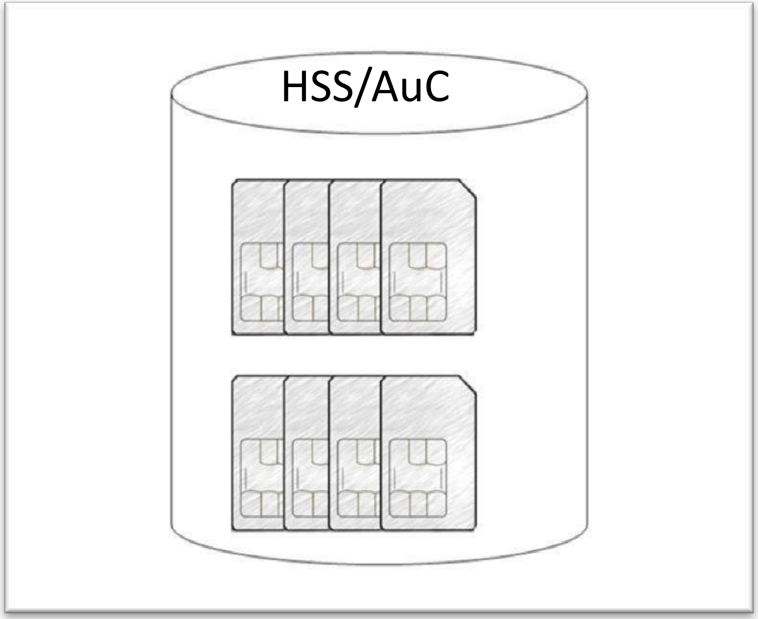
Jamming UE Radio Interface

- **Threat:** Jamming the LTE radio prevents the phone from successfully transmitting information.
  - Jamming decreases the signal to noise ratio by transmitting static and/or noise at high power levels across a given frequency band.
  - Research suggests that, due to the small amount of control signaling in LTE, this attack is possible.
  - Prevents emergency calls
- **Mitigation:** Unclear. Further research is required and may require changes to 3GPP standards to mitigate this attack.



Attacks Against the Secret Key (K)

- **Threat:** Attackers may be able to steal K from the carrier's HSS/AuC or obtain it from the UICC manufacturer:
  - Card manufacturers may keep a database of these keys within their internal network
- **Mitigation(s):**
  - Physical security measures from UICC manufacturer
  - Network security measures from carrier



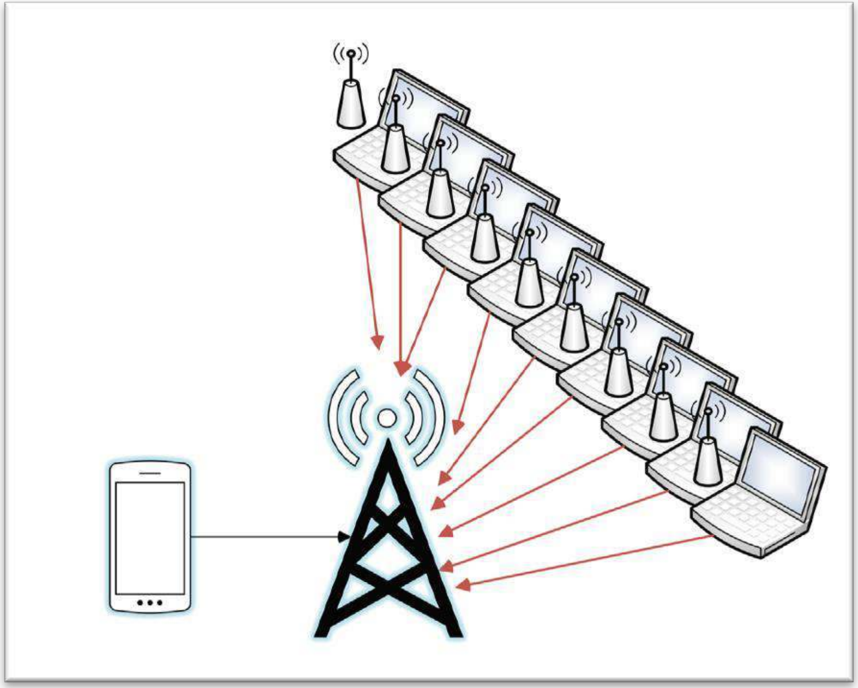
Physical Base Station Attacks

- **Threat:** The radio equipment and other electronics required to operate a base station may be physically destroyed

- **Mitigation:** Provide adequate physical security measures such as video surveillance, gates, and various tamper detection mechanisms

Availability Attacks on eNodeB & Core

- **Threat:** A large number of simultaneous requests may prevent eNodeBs and core network components (e.g., HSS) from functioning properly.
  - Simulating large numbers of fake handsets
- **Mitigation:** Unclear



End of the session