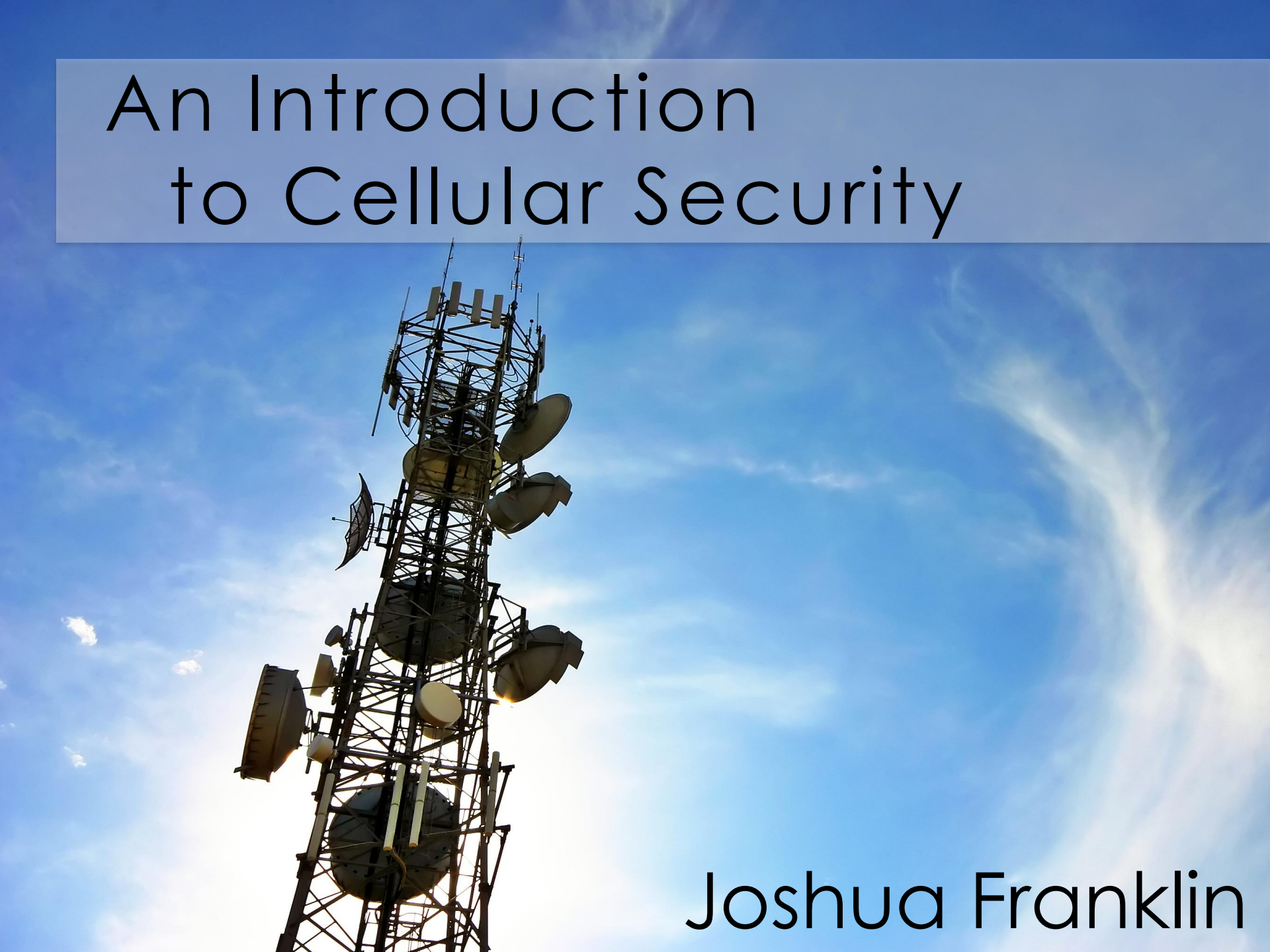
An Introduction to Cellular Security



Joshua Franklin

License

Creative Commons:
Attribution, Share-Alike

http://creativecommons.org/licenses/by-sa/3.0/

Introduction

- Cellular networks are a dense subject
  - This is not a deep dive
- The standards are large, complicated documents
- Involves physics, telecommunications, politics, geography, security…
- We will discuss older cellular networks first and build upon this knowledge
- The GSM, UMTS, and LTE standards are more or less backwards compatible
  - Major consideration during standards development

Who Am I?

- Joshua Franklin
- I hold a Masters in Information Security and Assurance from George Mason
  - Graduate work focused on mobile operating systems
- I work in election and mobile security

Learning Objectives

- Become familiar with the GSM, UMTS, and LTE family of cellular standards
- Be introduced to spectrum allocation and antennas
- Learn the security architecture of cellular networks
- Be introduced to how cellular networks have been hacked in the past

We will deeply explore LTE security while only touching on GSM and UMTS. LTE is the new standard moving forward (a.k.a., the new hotness). Previous cellular standards are being phased out.

Excluded Topics

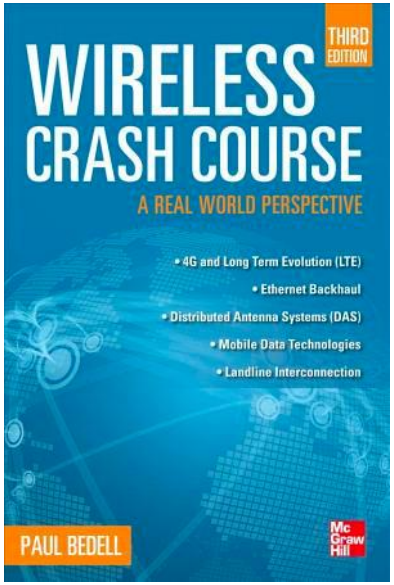
This class does not cover:

- Wireless physics
- Ancient wireless networks (AMPS, IMS, smoke signals)
- Wired systems (PSTN/POTS/DSL)
- Standards other GSM, UMTS, and LTE
  - CDMA2000, EV-DO, WiMax
- In-depth discussion of GPRS, EDGE, and HSPA variants
- SMS and MMS (text messaging)
- Mobile operating systems (iOS, Android, Windows Phone)
- QoS , Mobility management, and VoLTE
- Internetwork connections

Warning: This class is U.S.-centric but the standards are used worldwide. The network operators, frequencies, and implementations vary.

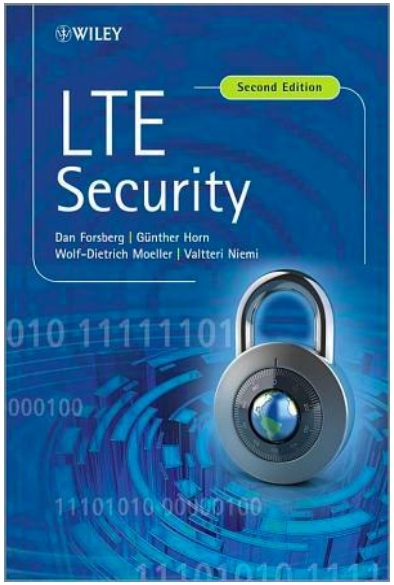
Books

Wireless Crash Course 3rd edition



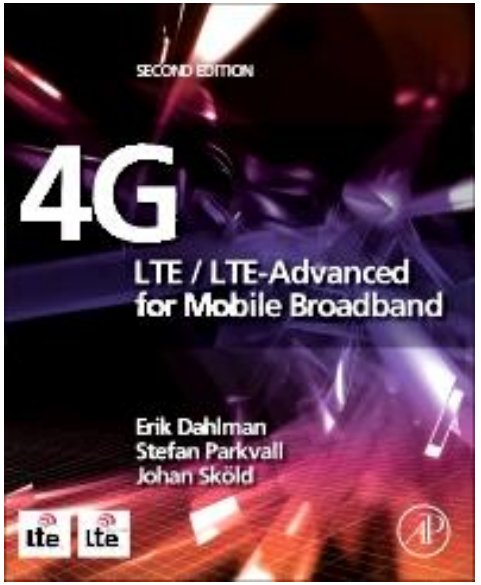
Easy Mode

LTE Security 2nd edition



Intermediate

LTE-Advanced for Mobile Broadband - 2nd edition



God Mode

Note: Many papers and presentations were also useful and are cited inline, but check the last slide for a complete listing.

Terminology

- Cellular standards use jargon and abbreviations frequently
  - LTE, EPS, BTS, K[ASME]
  - Nested acronyms are common
  - GERAN = GPRS Evolution Radio Access Network
  - LTE is often referred to as Evolved Packet System (EPS) in technical situations
- Learn to be comfortable with the jargon and acronyms
  - There is an associated glossary and cheatsheet
  - If something needs to be added or modified, please let me know
  - Especially to improve the course and associated documentation

Prerequisites

1. Basic understanding of networks and network protocols
2. Familiar with core cryptographic concepts
3. Basic knowledge of information security
4. Basic understanding of physics
5. Have made a phone call

There are no labs in this class

Agenda

- Wireless spectrum and cellular bands
- Important cellular concepts
- Overview of cellular standards
- Discussion of the following for GSM, UMTS, and LTE:
  - Network components
  - Security architecture (hardware tokens, authentication, cryptography)
  - Threats to these technologies
  - Notable attacks
- SIM Hacking
- Baseband Hacking
- Femtocells

What is LTE

- LTE is Long Term Evolution
- Fourth generation cellular technology standard from the 3rd Generation Partnership Project (3GPP)
- Deployed worldwide and installations are increasing
- All implementations must meet baseline requirements
  - Increased Speed
  - Multiple Antennas (i.e., MIMO)
  - IP-based network (All circuits are gone/fried!)
  - New air interface: OFDMA (Orthogonal Frequency-Division Multiple Access)
  - Also includes duplexing, timing, carrier spacing, coding...
- LTE is always evolving and 3GPP often drops new "releases"
  - This class is modeled around LTE-Advanced, but we won't dig deep enough to tell

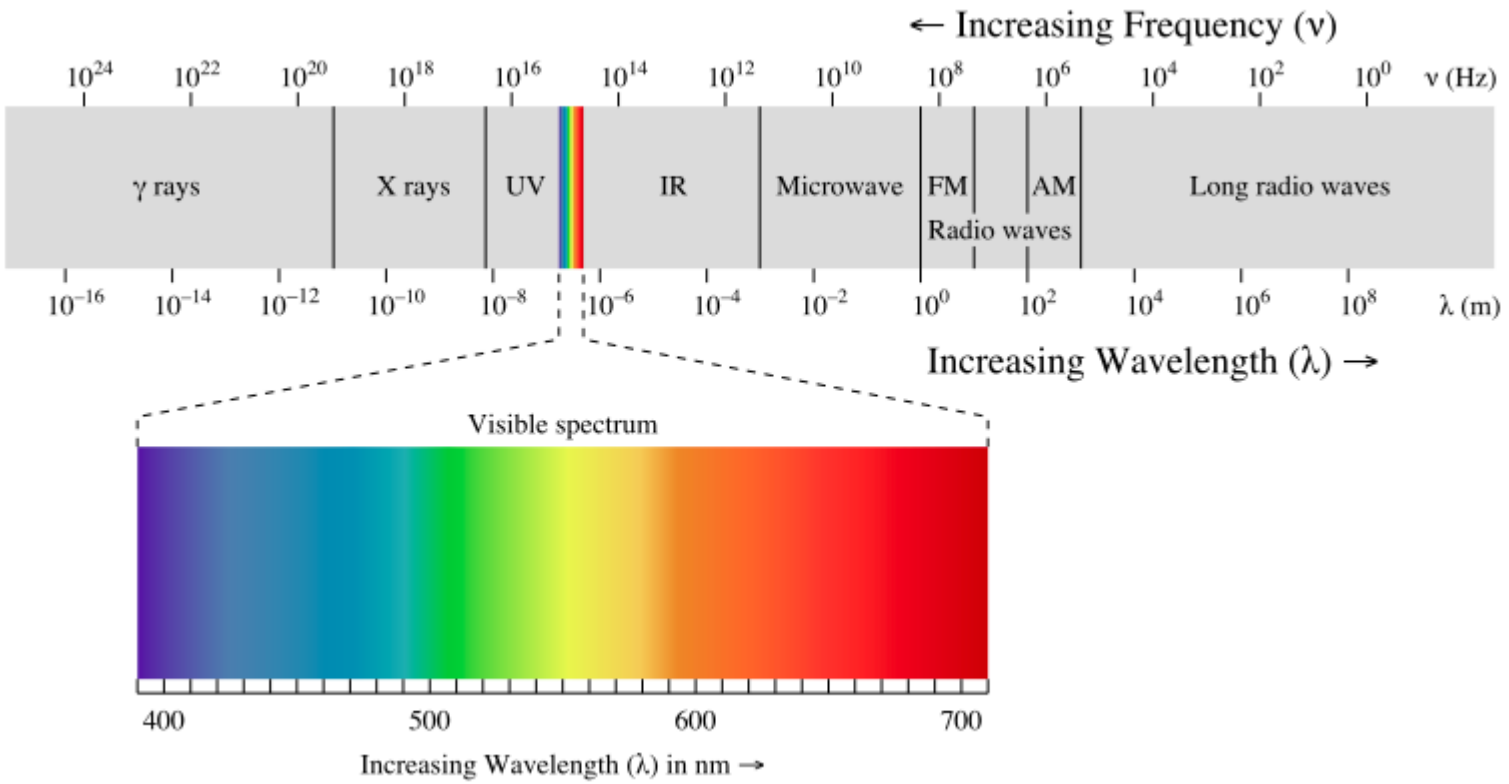
Cellular Network Operators

- Telecommunications company (telco)
  - Purchases spectrum
  - Builds out network (base stations and backhaul network)
  - Verizon, AT&T, T-Mobile, Sprint
- Mobile Virtual Network Operator (MVNO)
  - Does not have to purchase spectrum
  - Rents the towers but runs a distinct network
  - Cricket, Ting, MetroPCS, …

Radio Frequency Spectrum

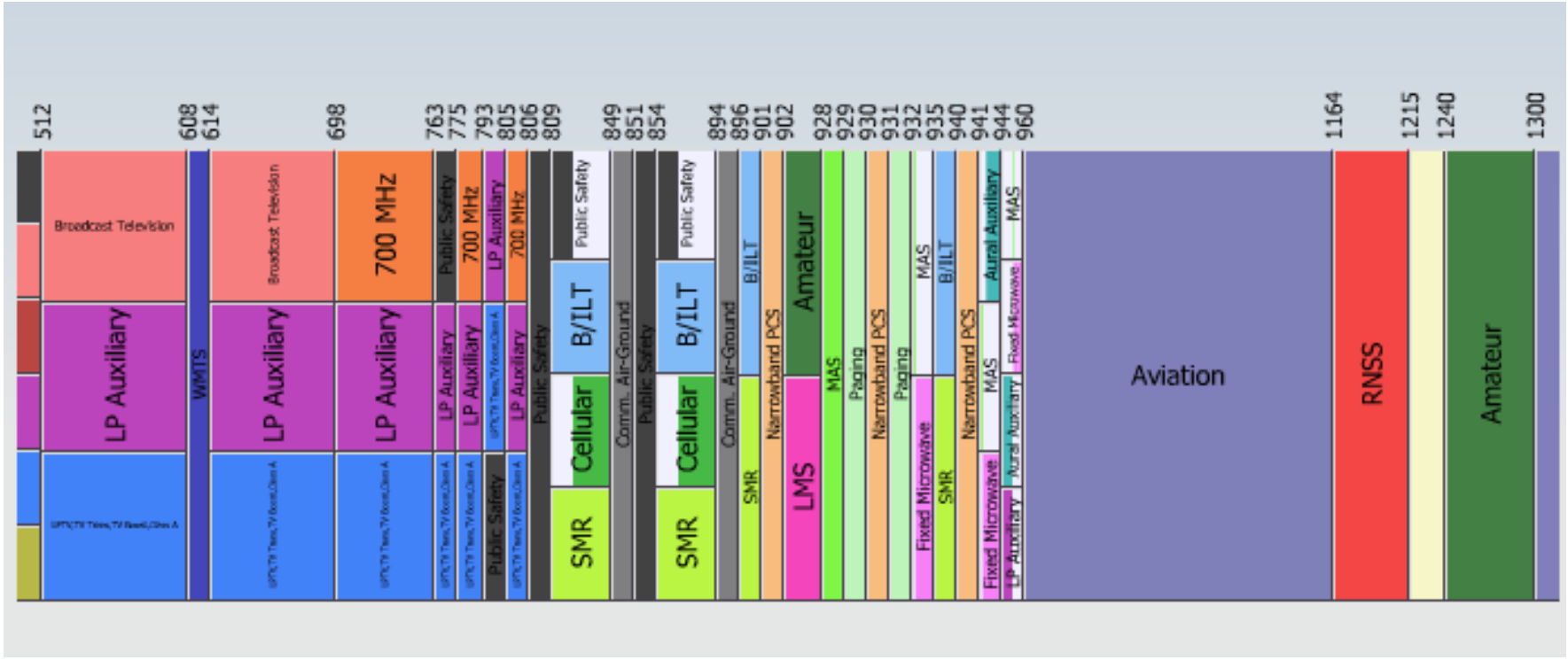
- Describes a range of frequencies of electromagnetic waves used for communication and other purposes
- RF energy is alternating current that, when channeled into an antenna, generates a specific electromagnetic field.
- This field is can be used for wireless communication
- Cellular spectrum ranges from 300 MHz to 3 GHz

EM Spectrum



Thanks to [Wikipedia]

Wireless Spectrum



From an interactive map available via the FCC

Popular Cellular Bands

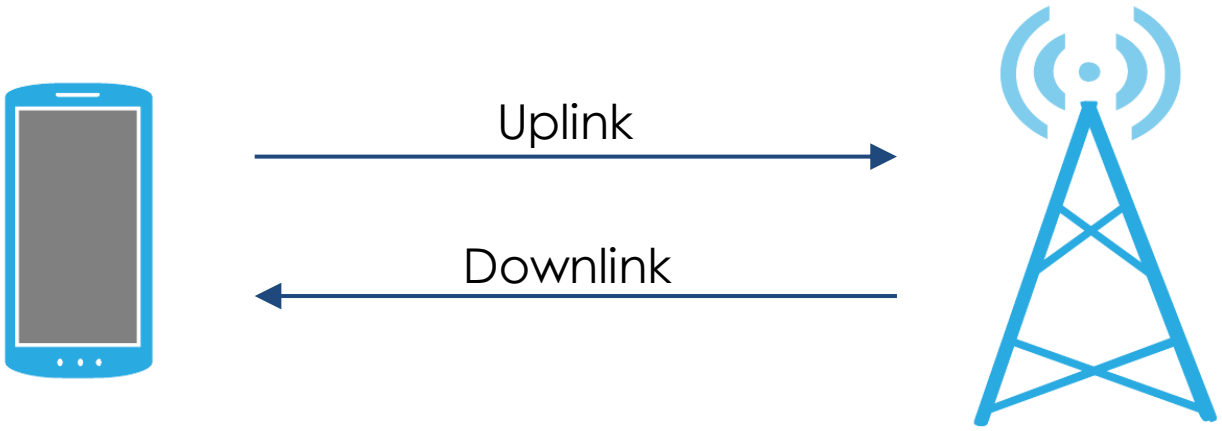
- 700 Mhz Band (Blocks A - E)
  - Considered uniquely useful to cellular activities
  - Verizon, US Cellular, AT&T and others own various portions
  - Will be used for 4G
  - Includes reserved spectrum for public safety
- 850 MHz
  - Great for cellular service
  - Easily bounces off objects
- 1900 MHz band (PCS)
- 2100 MHZ (Blocks A - F)
  - Mostly T-Mobile, but includes Cricket and MetroPCS
- This information changes periodically as spectrum is purchased & released

Chipset

- In the past, phones have typically been tied to a single carrier
- A phone's hardware is tied to a carrier based on many things (like the IMEI), but the major ones are the cellular standard and frequencies the carrier uses
- Phones are manufactured to work on specific radio frequencies
  - Specific chips needed for a given frequency range, thus chipset
- Nowadays, phones concurrently operate on many frequencies (and therefore networks)
  - Modern multi-band chips allow a single device to operate on multiple frequency ranges

Channel Allocation

- Typically there is a downlink channel and an uplink channel
- These channels needs to be spaced in frequency sufficiently far so that they do not interfere with each other

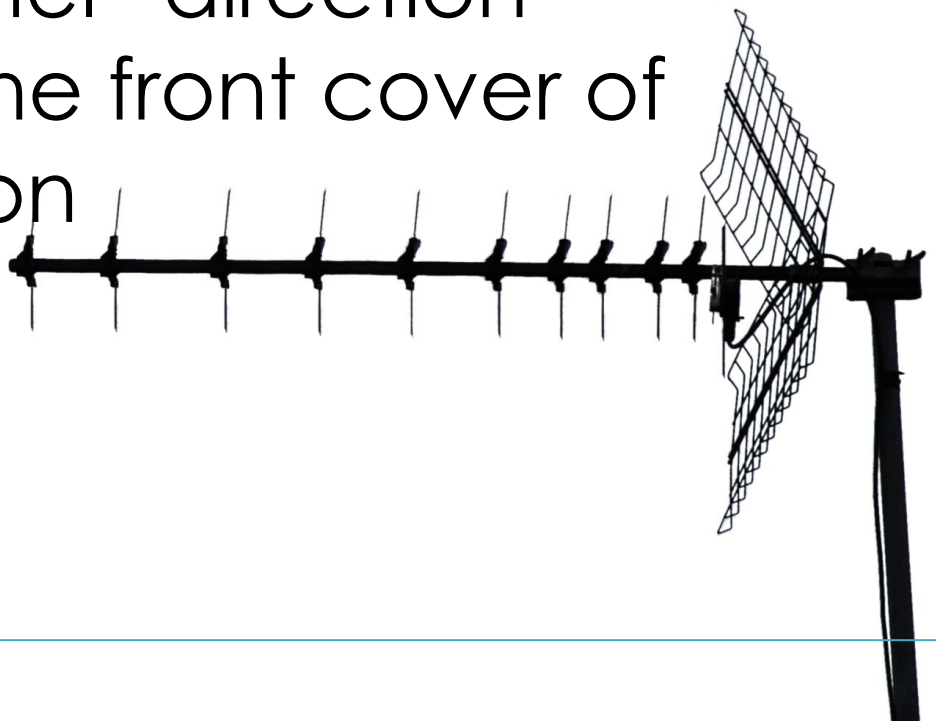


Antenna

- There are 2 main types of antennas, each with unique properties
- Omnidirectional
  - Emits energy in a spherical radius
- Directional
  - Emits energy in the shape of the antenna and in the direction and angle at which it is pointed

Directional Antenna

- Designed to radiate in a specific direction
  - The radiation is focused (see below)
- There are "panel" direction antennas on the front cover of this presentation



Omnidirectional Antenna

- Designed to radiate in across a specific plane
  - The radiation spreads outward from a center point
  - A donut is a reasonable visual

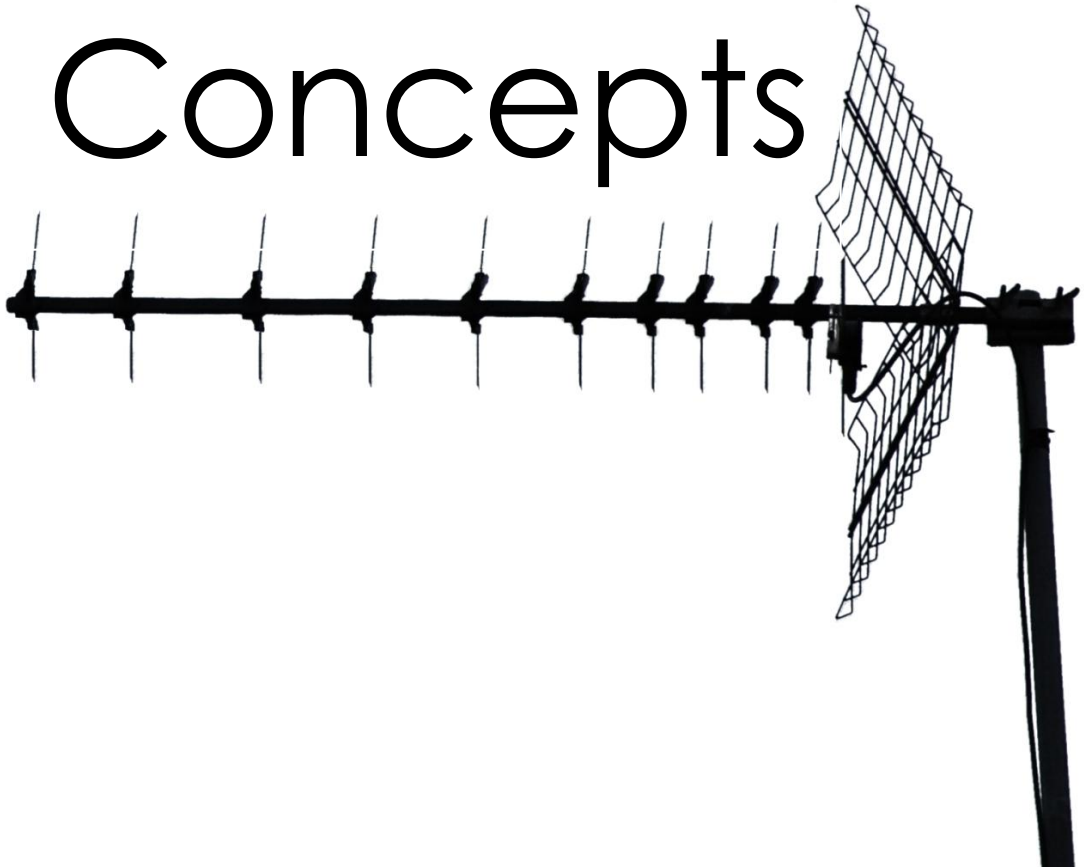
Device Antenna

- There are multiple antenna in your mobile device - although some are shared
- Designed to transmit and receive at various frequencies
  - Cellular (300 MHz - 3 GHz)
  - WiFi (Primarily 2.4 GHz, 5 GHz) [there are other odd frequencies specified]
  - Bluetooth (2400–2480 MHz)
  - NFC (13.56 MHz)

Multiple Antennas

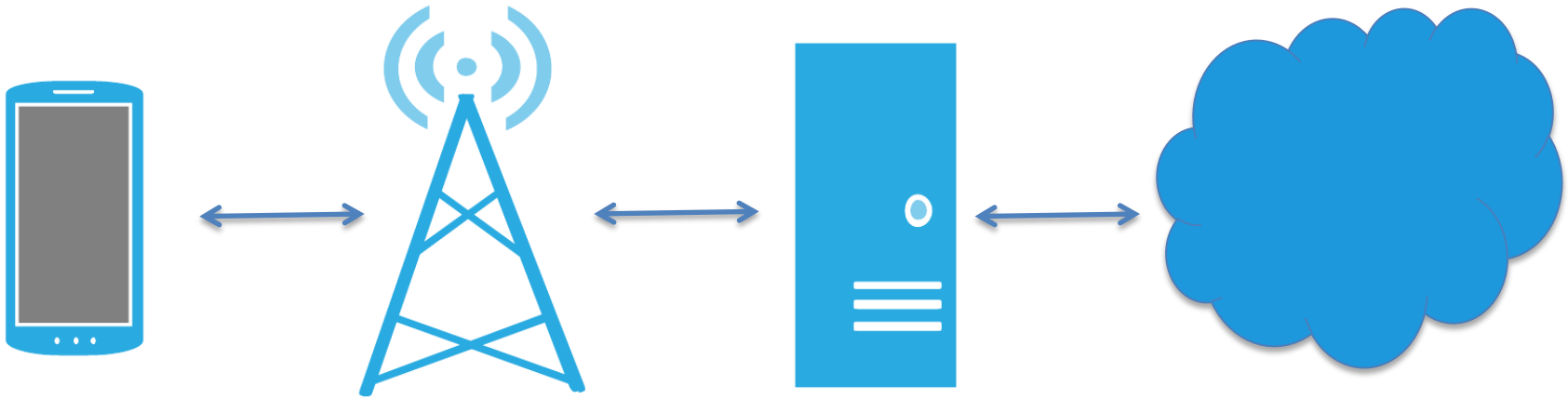
- LTE has a feature called Multiple-Input Multiple-Output (MIMO)
- Multiple antennas are on the mobile device and are used simultaneously to transmit and receive
  - Can significantly increase throughput
- Multiple types
  - Spatial diversity
  - Spatial multiplexing
- Further divided:
  - SISO - Single in, single out
  - SIMO - Single in, multiple out
  - MISO - Multiple in, single out
  - MIMO - Multiple in, multiple out

Important Concepts



Big Picture

Mobile devices (1) connect to a base station (2) which connects to a backhaul network (3), which connects to the internet (4).



Network Components

- The network between mobile devices and base stations is the Radio Access Network (RAN)
  - This name slightly changes with new standards
- Base stations are permanent cellular sites housing antennas
- Base stations and the backhaul network are run by telco, but there are interconnections and shared sites
  - AT&T customers need to be able to contact Verizon (vice versa)
- Base stations often connect to backhaul via wired technologies (i.e., fiber)
  - Base stations often communicate with each other via wireless

Mobile Devices

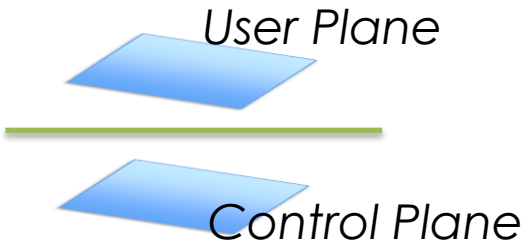
- These are the devices with wireless radios that connect to cell towers
  - Radios are inside phones, tablets, laptops, etc. . .
- LTE uses the term User Equipment (UE), previously ~ Mobile Station (MS)
- The parts of the UE we are concerned with:
  - The handset, aka the ME (Mobile Equipment)
  - USIM (Universal SIM)
  - Baseband processor

Baseband

- Typically a separate processor on the phone
  - From companies like Qualcom, Infineon, etc.
- Handles all of the telecommunications-related functions
  - Sends, receives, processes signals
  - Base station and backhaul network communication
  - Has direct access to microphone, speakers…
- Runs a real time operating system (RTOS)
  - Performance matters!
  - OSs include ThreadX, Qualcomm's AMSS w/ REX kernel, OKL4
- Sometimes shares RAM with application processor (baseband as a modem), sometimes each processor has distinct RAM(shared architecture)
  - In a shared configuration the baseband is often the master
- May be virtualized

Planes of Communication

- Many control systems divide communication into two planes - one for processing information from users and another for how to setup/breakdown the channel and other important functions
- Think of this similar to how FTP uses two ports
  - TCP port 20 - data
  - TCP port 21 - control
- Control Plane (CP)
  - A private communication channel that is distinct from data the UE operator can influence
  - Used to send control messages to components
  - Mobile users should not be able to influence this in any way
- User Plane (UP) signaling
  - Voice and data information
- Cellular networks use this design extensively



Packets and Circuits

- Pre-LTE, cellular networks used circuit switching technology for voice
  - LTE uses VoLTE which is VoIP over LTE
  - Not implemented currently, calls fall back to previous networks
- Data traffic is sent over nearly distinct interconnected packet switching networks
  - GSM first used GPRS, then moved to EDGE
  - UMTS used HSPA technologies including HSPA+
- Since LTE is completely IP based, it does not use circuits
- We're not there yet, but soon.

Network Interconnection

- Circuit switched networks need to be able to connect with packet switched networks and other distinct cellular networks
  - The internet is a good example
  - This is a complex process
- GPRS (General packet radio service)
  - 2.5G packet switched technology
- EDGE (Enhanced Data Rates for GSM Evolution)
  - 2.75G packet switched technology
- HSPA (High Speed Packet Access)
  - 3.5/3.75 packet switched data technology
  - There were a few quick iterations on this technology, thus "variants"

Attachment, Handoff, & Paging

- The first step in a mobile device connecting to a network is referred to as network attachment
  - Mobile devices request network access to a base station, which passes this request onto the backhaul network
  - Authentication of the mobile device is then performed
- If a mobile device is moving (such as on a freeway) a call will need to be transferred from one base station to another
  - This is called handoff
  - This is a very common, yet is complex, process
- Paging is the process of how a backhaul network locates and directs calls a mobile device
  - Base stations provide a list of active devices to the backhaul

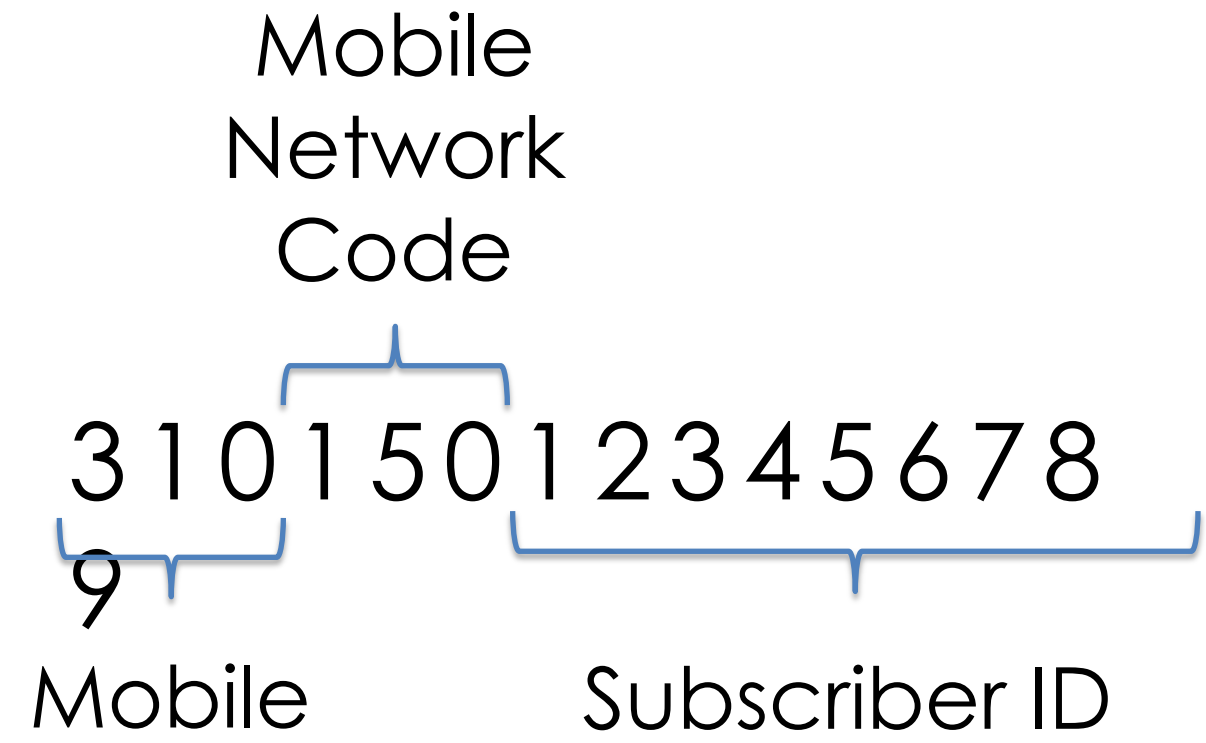
Connection Management

- EPS Connection Management (ECM)
- UE related information is released after a certain period of time without use or connection
- ECM-states
  - ECM-CONNECTED
  - ECM-IDLE
- TS 23.401for more information

Subscriber Identity

- GSM, UMTS, and LTE all contain a unique ID for a cellular subscriber
  - International Mobile Subscriber Identity (IMSI)
  - 15 digit number stored on the SIM
- Consists of 3 values: MCC, MNC, and MSIN
  - Possibly a software version (SV) appended (IMSI-SV)
- Mobile Country Code (MCC) - Identifies the country
- Mobile Network Code (MNC) - Identifies the network
- Mobile Subscriber ID number (MSIN) - Identifies a user
- Temporary identities also exist
  - Temporary Mobile Subscriber Identity (TMSI)
  - Globally Unique UE Identity (GUTI)
- This information is stored on the SIM/USIM
- Mobile Subscriber ISDN Number (MSISDN) – The phone number, which is distinct from the MSIN

IMSI Example



The MNC may be 2 or 3 digits, depending on region. 3 is common in the USA while 2 is common in Europe.

Thanks to Wikipedia for the sample IMSI

Terminal Identity

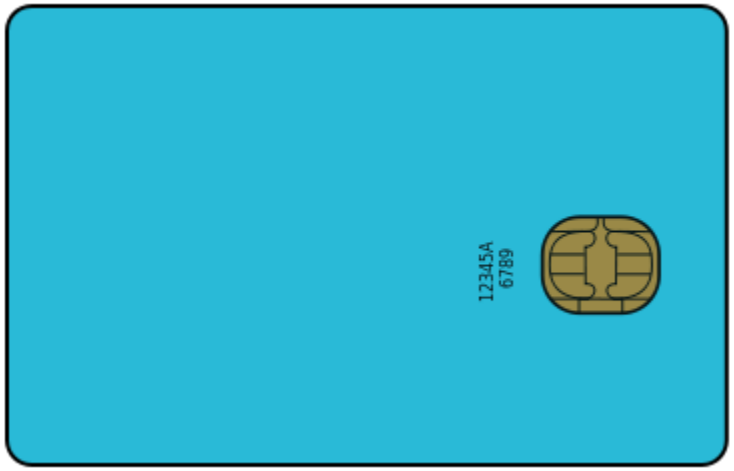
- GSM, UMTS, and LTE all contain a unique ID for a terminal ME/UE
  - International Mobile Equipment Identity (IMEI)
- It is16 digits with the first 14 indicating equipment identity
  - The last 2 indicates software version (SV)
  - Referred to as IMEISV
- Dial *#06# to display your IMEI
- Illegal in some countries to change a phone's IMEI

SIM Cards

- A removable hardware token used for GSM, UMTS, and LTE
  - Verizon is changing to LTE and is also using the hardware token
- Over 7 billion SIMs in circulation
- Houses a processor and runs an OS
- Java Card runs atop the OS, which is a type of Java Virtual Machine (JVM) for applications
- Stores cryptographic keys and sometimes SMSs and contacts
- SIM application toolkit (STK) is used to create mobile applications
- SIMs are deprecated – the modern term is USIM
  - The USIM runs atop the UICC which is the physical card

SIM Card

Full-size SIM



Micro-SIM

Mini-SIM

Nano-SIM

From left to right, we are only removing plastic. The integrated circuit remains static.

Thanks to Wikipedia

Threats to Cellular Networks

- The communication medium is open and accessible by all – Jamming and femtocells
- SIM Cloning
  - Copying a phone's unique information to steal another customer's service
  - Cloning is not as common today
- Threats to Privacy
  - Cellular networks need, or be able to quickly locate, where the a mobile device is at all times
- Battery life
  - Pay phones don't need to be charged once a day
- Mobile network operators have a large and complex network to defend

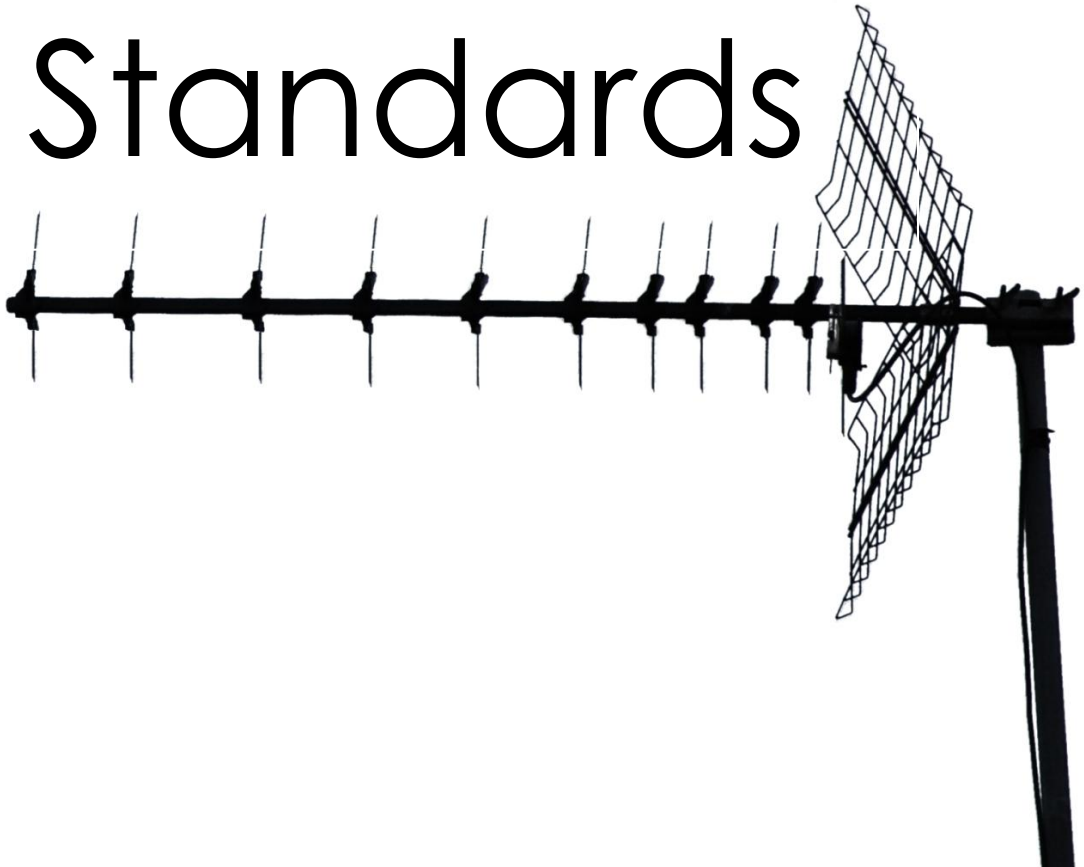
Jamming

- Cellular devices send information via radio transmissions
  - Interrupting these transmissions is called jamming
- It is possible to jam a large frequency range, such as all GSM traffic in an area, or only specific frequencies, like those used for control signals
- 3GPP standards state that jamming attacks are outside of their threat model
- You can buy jammers online, and depending on the range and power requirements, they can be quite cheap
  - Beware the wrath of the FCC, other three letter agencies, and your local law enforcement

Femtocells

- Femtocells are small extensions of the cellular network - often for personal or business use
  - Technically the standard refers to them as Home Node B (HeNB)
  - Limited range and relatively affordable
- They may be provided by telcos if requested and of course you pay for this convenience
  - The purchaser (often the user) does not have full administrative control of the device, similar to set-top boxes
  - *The purchaser has complete physical access*
- These devices introduce many new threats
  - Customers retain physical control and can perform offline attacks
  - Attacks on the core network through the femtocell
  - Jamming requires less power because an attacker can be closer
  - Attackers can quickly set one up in new location to attract UEs

Cellular Standards



3GPP

- An international standards body
- Evolves and/or standardizes GSM, UMTS, LTE among others
- From their page:

The 3rd Generation Partnership Project (3GPP) unites [Six] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), known as "Organizational Partners" and provides their members with a stable environment to produce the highly successful Reports and Specifications that define 3GPP technologies

- We will primarily discuss 3GPP standards
- Other standards exist from a distinct standards body known as 3GPP2
  - CMDA2000 and the now deprecated UMB

Major Standards

- Multiple standards bodies involved
- Standards grow and evolve from one another

- GSM
- CDMA
- UMTS
- EV-DO
- WiMAX
- LTE

Cellular Standards

Generation	3GPP Circuit Switched	3GPP Packet Switched	3GPP2	Wimax Forum
2G	GSM		cdma One	
2.5G		GPRS		
2.75G		EDGE		
3G	UMTS		CDMA 2000	
3.5G		HSPA/+	CDMA EV-DO	
4G		LTE	~~UMB~~	WiMAX

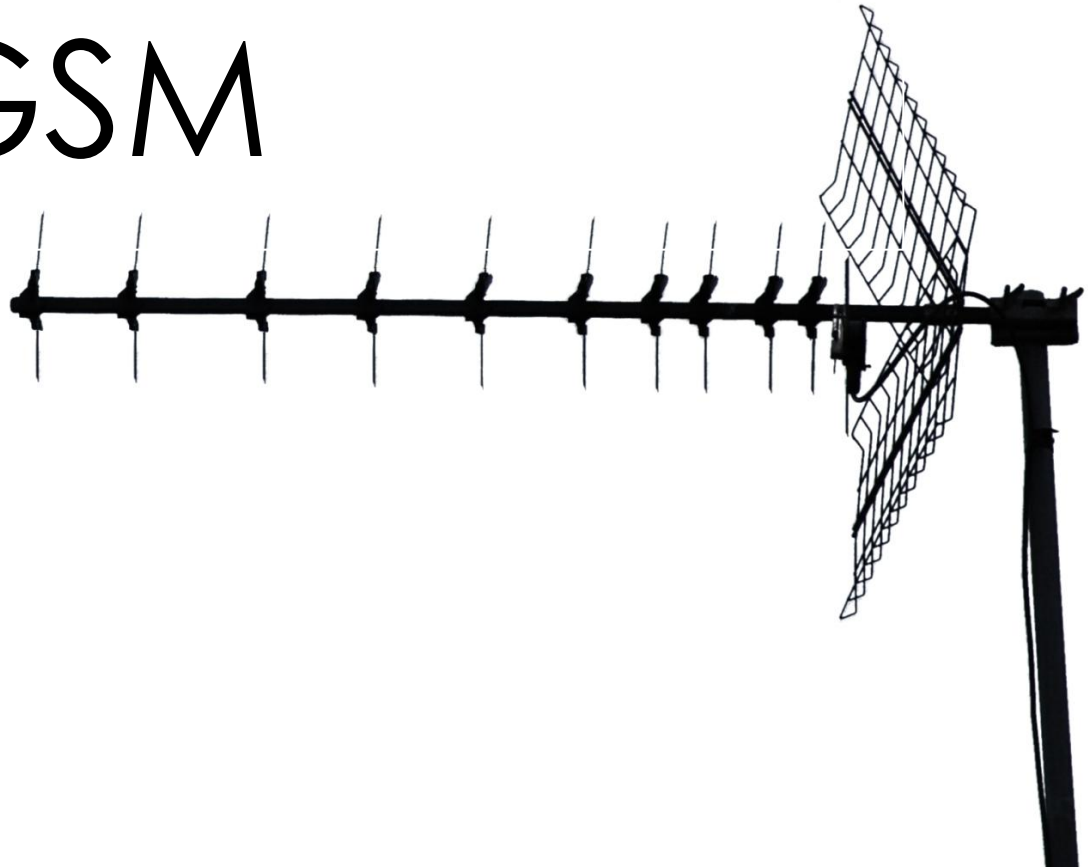
A Note on 3GPP

- LTE is a 3GPP specification
  - Therefore we will be discussing 3GPP specifications in depth
- We will introduce GSM and associated security issues
- We will then build on these concepts from GSM to UMTS to LTE
- Packet switched technologies will be discussed as well
- 3GPP2 and WiMax Forum standards are not included

LTE Security Architecture

- The primary 3GPP standard governing LTE is TS 33.401
  - Get to know it
  - Other standards exist and are referenced
- I link to the overarching page for the standard so the most recent version of the standard is attainable
  - Download and extract the zip for the word document

GSM



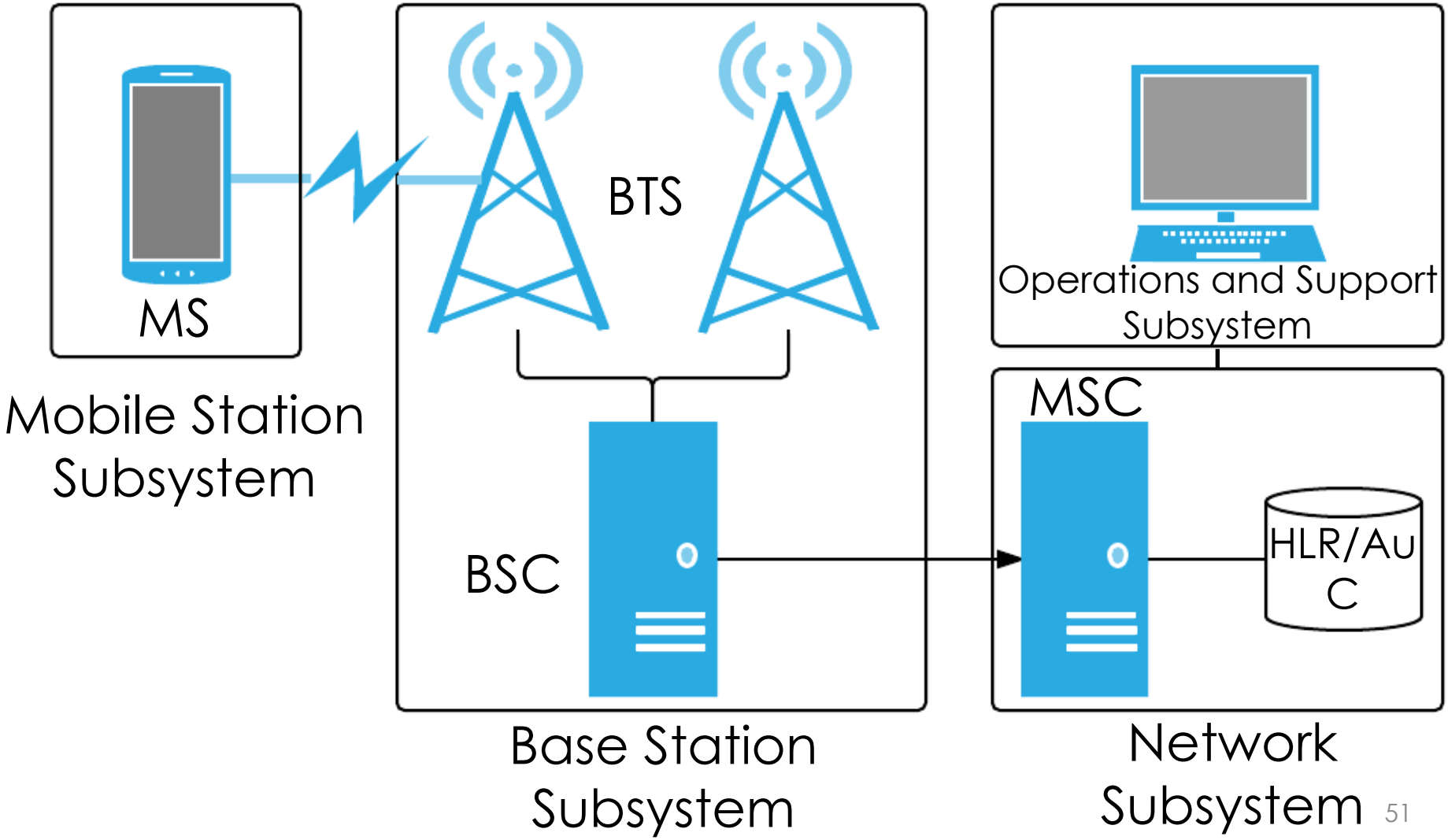
GSM

- Global System for Mobile Communications
- 2G digital voice
- Air interface: TDMA
  - Multiple users on the same channel
- Operates at various spectrums worldwide
- There are 4 separate systems:
  - Base station subsystem (BSS)
  - Network subsystem (NSS)
  - Operations and support subsystem (OSS)
  - Mobile station subsystem (MSS)
- Each subsystem has a distinct purpose

GSM Component Description

- Mobile station subsystem (MSS)
  - Mobile handset and SIM
- The base station subsystem BSS consists of a controller and transceiver
  - Base station transceiver (BTS) is the cell tower
  - Base station controller (BSC) controls 1 or more BTSs
  - Housed at the Mobile Telephone Switching Office (MTSO)
- Network subsystem (NSS):
  - MSC (Mobile Switching Center) and MTSO
  - MTSO-switch connects cell network to PSTN
  - MTSO houses the HLR, which supports the AuC
- Operations and Support (OSS)
  - Manages the network as a whole

GSM Architecture Diagram



GSM Security Design

- Meant to achieve equivalent or greater security than wired systems of that time
- Security mechanisms should not have a negative impact on the system
- Primary security mechanisms:
  - Subscriber authentication
  - Privacy achieved via temporary identities
  - Encryption of the Radio Area Network and backhaul
  - ME to BTS and BTS to MMC - using a key known as Kc

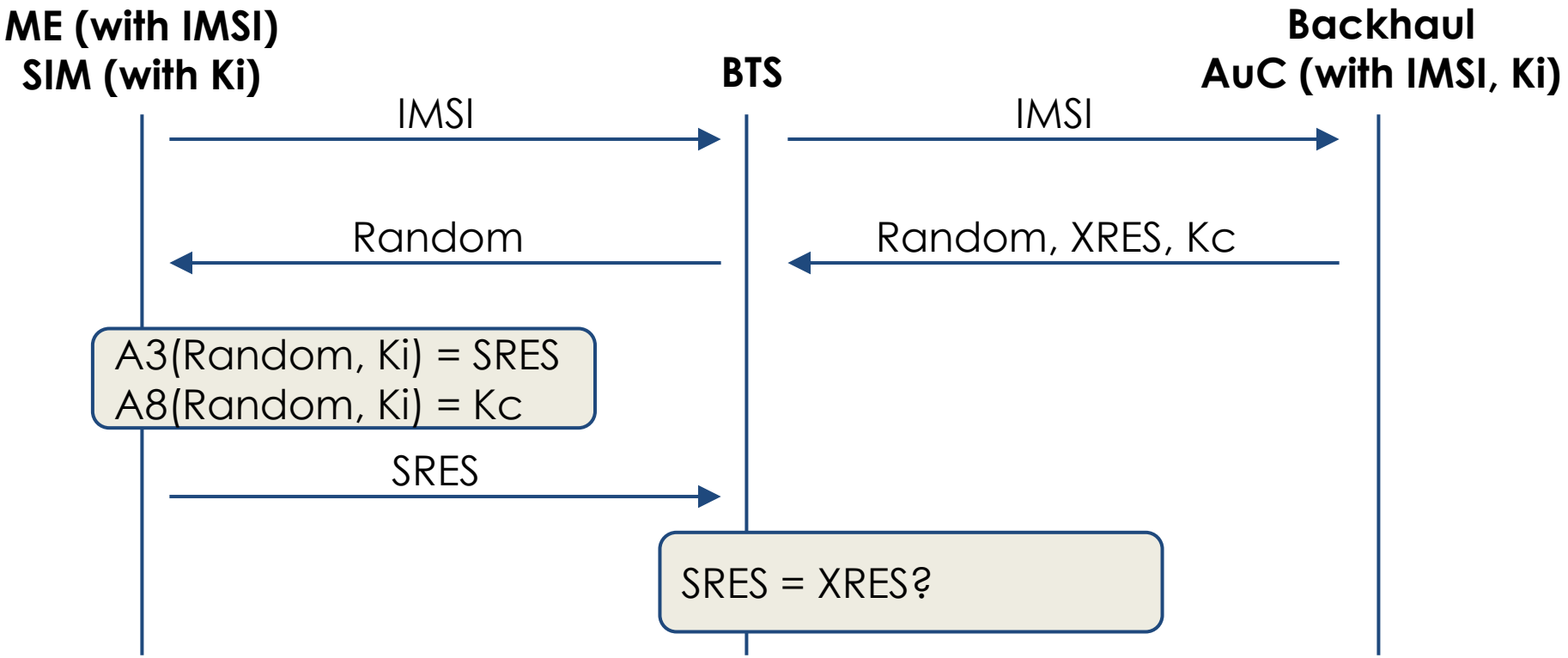
GSM SIM

- Tamper resistant hardware token
- Stores 128-bit key, called Ki, which is used to derive Kc
  - Ki never leaves the card
  - Also stored in AuC
- Contains key generation software
- Subscribers are authenticated to the network by proving knowledge of Ki
  - How? The Authentication and Key Agreement (AKA)

GSM AKA

- AKA is a challenge and response authentication protocol
  - Authentication is not mutual
- A devices IMSI is sent to the BTS, which is passed to the HLR/AuC
- The HLR/Auc sends the Kc, 128-bit random number, and an Expected Response (XRES) to the BTS
  - Kc is a session encryption key
- The BTS passes the random number to the ME
- The ME uses the Ki and the random number to arrive at Kc and provides the BTS with an SRES
- The BTS checks if SRES is equal to XRES
  - If so they subscriber is authenticated
- The BTS provides the ME with an encrypted Temporary Mobile Subscriber Identity (TMSI)
  - Not always encrypted

GSM AKA Ladder Diagram



GSM Cryptographic Algorithms

- Families of algorithms: A3, A5, and A8
- A3 is used for subscriber authentication to derive XRES
- A5 is used to encrypt data in motion such as radio encryption
  - ME to BTS
  - A5/0 – no encryption
  - A5/1, A5/2, and A5/3 are 64-bit stream ciphers
  - A5/4 is a 128-bit stream cipher
  - An efficient attack exists against A5/2 and it is deprecated
- A8 is used to derive the 64-bit symmetric key, Kc
  - The final 10 bits are zeroes
- The A3 and A5 families are non-standardized
  - They only need to be on devices and equipment owned by the carrier (USIM, BTS, backhaul)
  - MILENAGE is provided if needed

Note: GPRS and EDGE use different algorithms

MILENAGE

- Set of five cryptographic one-way functions specified by 3GPP
  - Usage is optional as telcos can specify their own
  - Block ciphers with 128-bit key
  - GSM, UMTS, and LTE
- Used during AKA for key and parameter generation
  - We will explore this further during the LTE segment
- These are the ‘f boxes’ (f1, f2, f3, f4, f5)[Nyberg04]

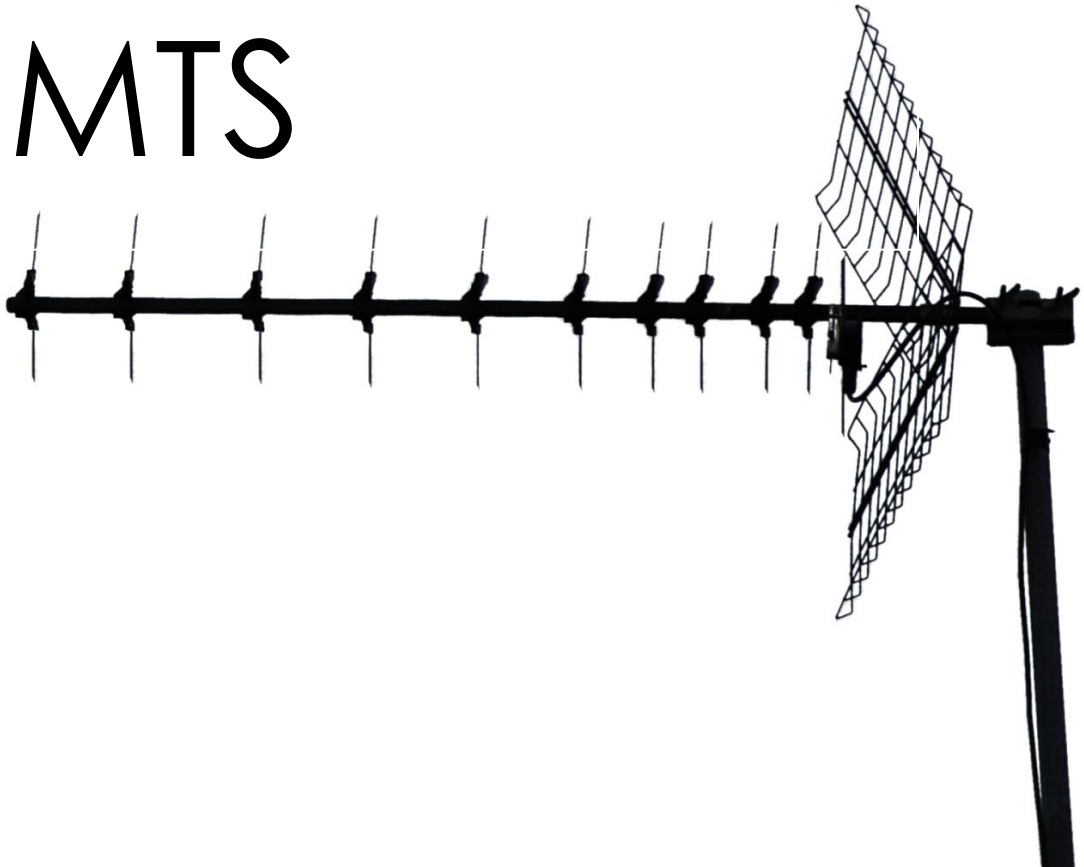
Threats to GSM

- Cryptography-based
  - Short 64-bit keys
  - A5/2 efficient attack
  - A5/1 attack with large amounts of plaintext
    - Implementation flaw exists [Hulton08]
- Weak cipher renegotiation and null cipher attacks possible
- SIM cloning
- Man-in-the-Middle (MitM) attack via rogue base station (femtocell)
  - During AKA, the handset cannot authenticate the network
- Only radio traffic is encrypted - once information is in the backhaul it is cleartext [Hulton08]
- IMSI sometimes sent in the clear [Hulton08]
- Some control signaling may be unprotected

Notable Attacks

- Hulton et al, Blackhat 2008
  - Showed how to intercept GSM signals with software defined radio
  - Showed a practical method to crack A5/1 (as did Karsten Nohl)
- Paget, Defcon 2010
  - Demonstrated a homegrown GSM BTS
  - Intercepted calls

UMTS



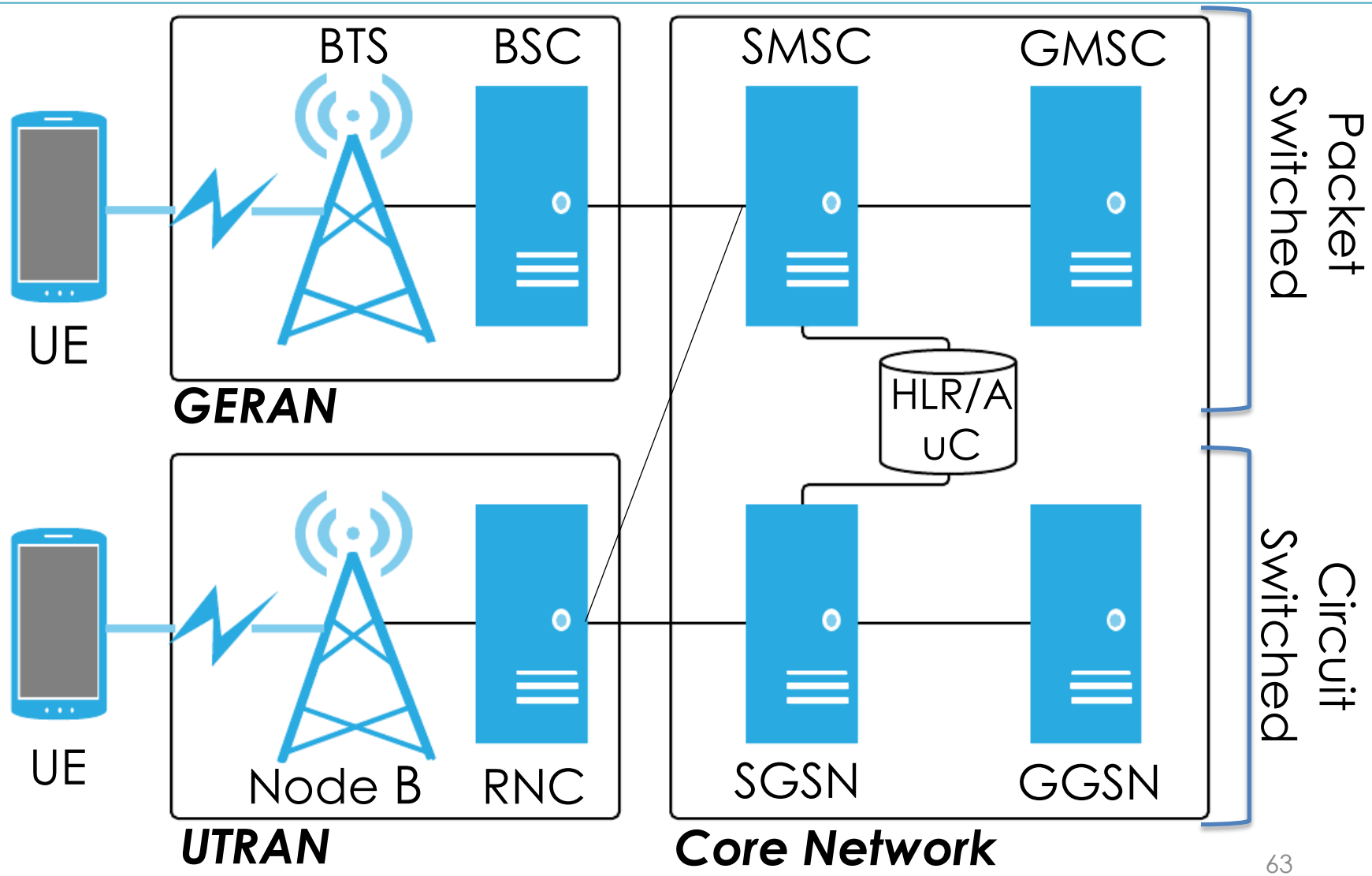
UMTS

- Universal Mobile Telecommunications System
- 3G digital voice
- Air interface: W-CDMA
- Operates at various spectrums worldwide

UMTS Components

- Consists of the core network (CN), Universal Terrestrial Radio Access Network (UTRAN), and UE
- Runs 2G packet switched and 3G circuit switched components concurrently - it looks confusing at first
- The UTRAN contains:
  - Node B (think of the phone as Node A)
  - Radio Network Controller (RNC)
- The CN contains:
  - Serving Mobile Switching Center (GMSC)
  - Gateway Mobile Switching Center (GMSC)
  - Serving GPRS support node (SGSN)
  - Gateway GPRS support node (GGSN)
  - Home Location Register/Authentication Center (HLR/AuC)
- We are not discussing GPRS-related nodes

UMTS Architecture Diagram



UMTS & GSM Compatibility

- UMTS was designed to work concurrently with GSM
- 2G SIMs were included
- Much of the terminology is slightly modified
  - BTS -> Node B

UMTS Security Design

- Iterative enhancement on GSM security
- Enhanced AKA
- New confidentiality and integrity cryptographic algorithms
- Introduction of Network Domain Security for IP-based protocols (NDS/IP)
  - IPSec

UMTS Hardware Token

- The GSM SIM now labeled the USIM
  - USIM application runs atop the UICC
- Contains a new hardware protected 128-bit key: K
  - As in GSM, never moves from UICC and HLR/AuC
  - Keys are derived from K as needed
  - HLR/AuC stores an IMSI and K per subscriber

UMTS AKA

- Similar to GSM - challenge & response protocol
  - UE proves knowledge of a key
  - UE somewhat authenticates the home network
  - Femtocells can still create a fake connection
  - New algorithms (f1 through f5 and f1* through f5*)
  - AKA algorithms are network specific and don't need to be standardized
- UE gains assurance that confidentiality key (CK) and integrity key (IK) were generated by the serving network
  - True serving network authentication is not achieved
  - Man in the middle still possible

UMTS Cryptography

- Completely public algorithms
- Increased key-length to 128-bits
  - Yay!
- Two new families of algorithms
  - UMTS Encryption Algorithm 1 and 2 (UEA1, UEA2)
  - UMTS Integrity Algorithm 1 and 2 (UIA1, UIA2)
- UEA1 and UIA1 are based on KASUMI
  - Block-cipher related to AES
- UEA2 and U1A2 are based on SNOW 3G
  - Stream cipher

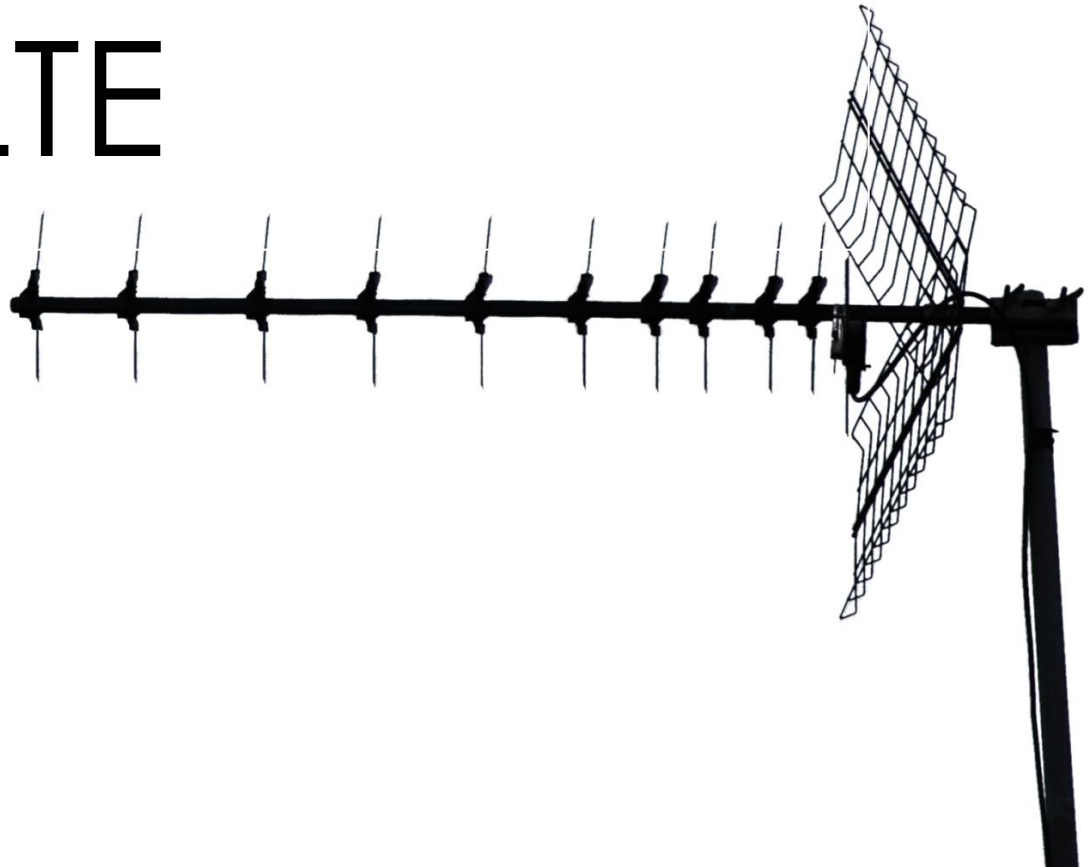
UMTS NDS/IP

- Provides protection for control-plane traffic, including authentication and anti-replay
  - Enter NDS/IP
  - Typically does not apply to user plane traffic
- A security domain under control of mobile network operator
- Certain connections between components may not be protected due to optional requirements in 3GPP standards
- Can internetwork with external NDS domains

Threats to UMTS

- Cryptography-based
  - There are many attacks against KASUMI [Kühn 2001, Dunkelmann and Keller 2008, Jia et al. 2011, Dunkelmann et al. 2010]
  - Attacks against Snow 3G [Brumley et al. 2010, Debraize and Corbella 2009]
- Backward compatibility
  - When a GSM SIM is used in UMTS only 64-bit keys are used
- IMSI catchers during AKA process
- U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS," in ACM WiSec, 2004, pp. 90–97

LTE



LTE

- Long Term Evolution
  - Also known as the Evolved Packet System (EPS)
- 4G data **and** voice technology
- Air interface: OFDMA
- 3 main components:
  - Evolved U-TRAN (E-UTRAN) - Radio Network
  - Evolved Packet Core (EPC) - Backhaul
  - IP Multimedia Subsystem (IMS) - Extended backhaul functionality
- Remember: LTE is a completely packet-switched technology for both data and voice
  - LTE currently falls back to older networks for voice (Circuit-switched fallback)
- VoLTE (voice over LTE) is in the works
  - I'll likely need to update this bullet in a year

LTE Security Requirements 1

- EPS shall provide a high level of security
- Any security lapse in one access technology must not compromise other accesses
- EPS should provide protection against threats and attacks
- Appropriate traffic protection measures should be provided
- EPS shall ensure that unauthorized users cannot establish communications through the system
- EPS shall allow a network to hide its internal structure from the terminal
- Security policies shall be under home operator control
- Security solutions should not interfere with service delivery or handovers in a way noticeable by end users
- EPS shall provide support lawful interception

LTE Security Requirements 2

- Rel-99 (or newer) USIM is required for authentication of the user towards EPS
- USIN shall not be required for re-authentication in handovers (or other changes) between EPS and other 3GPP systems, unless requested by the operator
- EPS shall support IMS emergency calls
- EPS shall provide several appropriate levels of user privacy for communication, location and identity
- Communication contents, origin and destination shall be protected against disclosure to unauthorized parties
- EPS shall be able to hide user identities from unauthorized parties
- EPS shall be able to hide user location from unauthorized parties, including another party with which the user is communicating

High-Level Threats to LTE

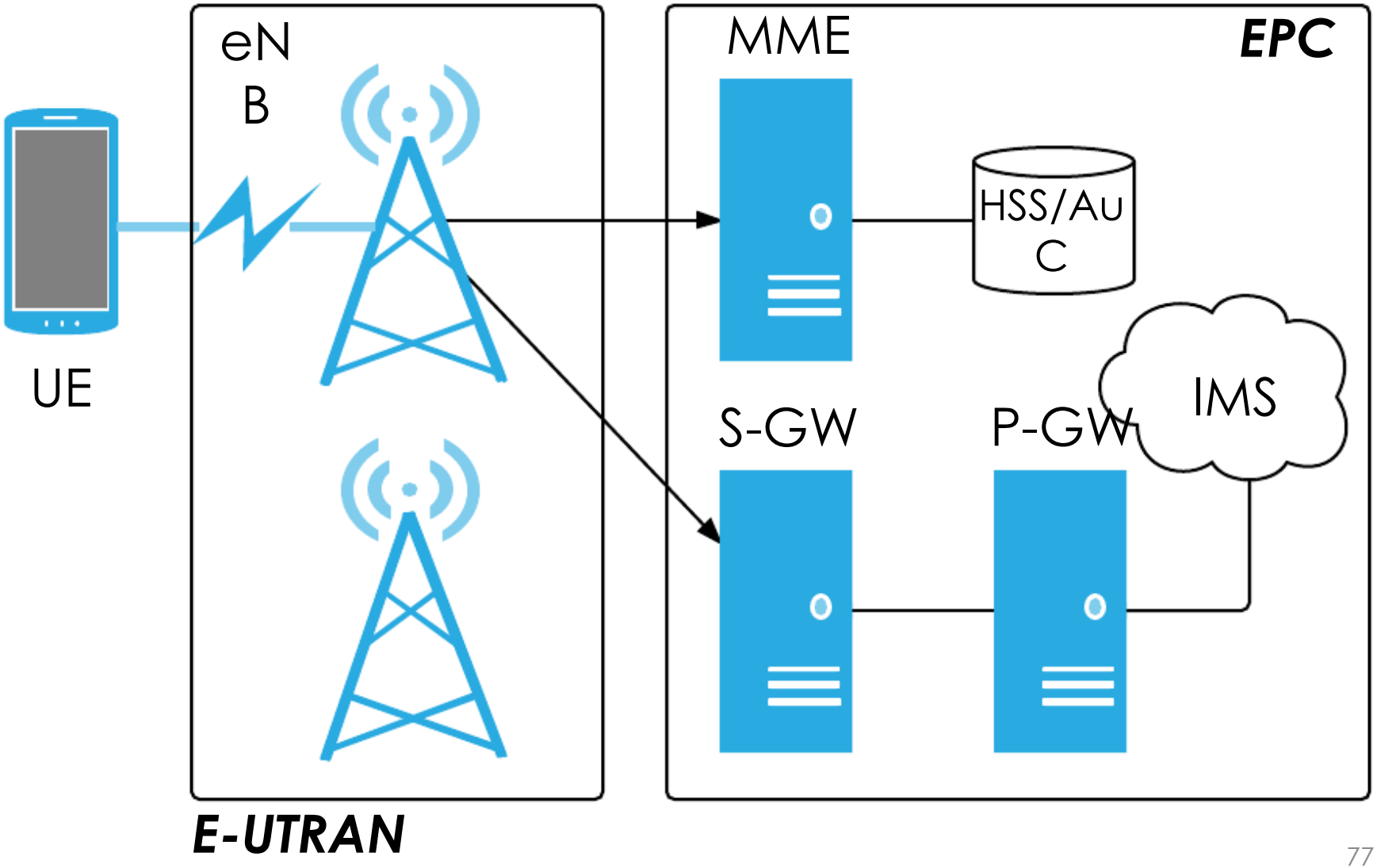
- Tracking identity, privacy or devices
- Jamming handsets or network equipment or other attacks on availability
- Physical attacks on base stations or network equipment
- Manipulating control plane or user plane data
- Threats related to interaction between base stations, or dropping to older standards or other networks

Jamming attacks are not within the threat model of LTE

LTE Components

- User equipment (UE)
- Evolved Node B (eNodeB)
- Mobility Management Entity (MME)
- Serving Gateway (S-GW)
- Packet Data Network Gateway (P-GW)
- Home Subscriber Server (HSS)

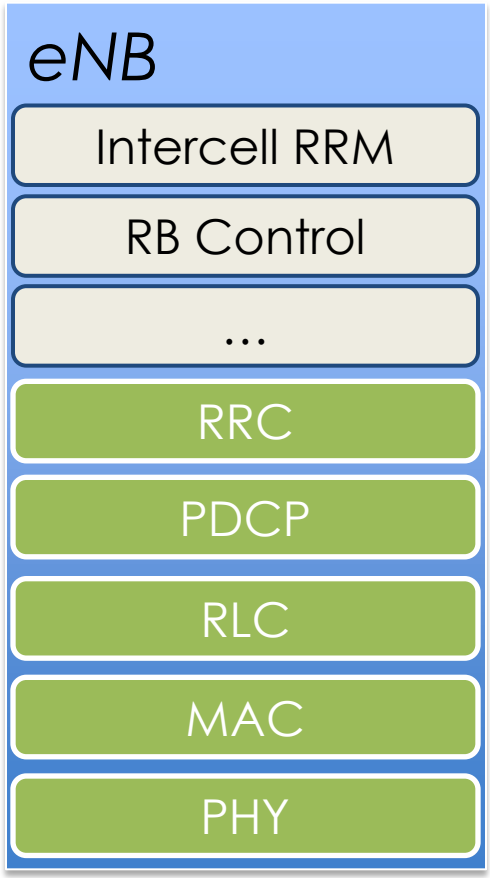
LTE/EPS Architecture Diagram



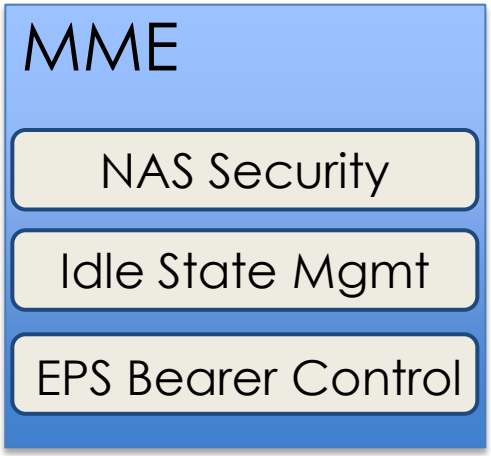
Component Descriptions

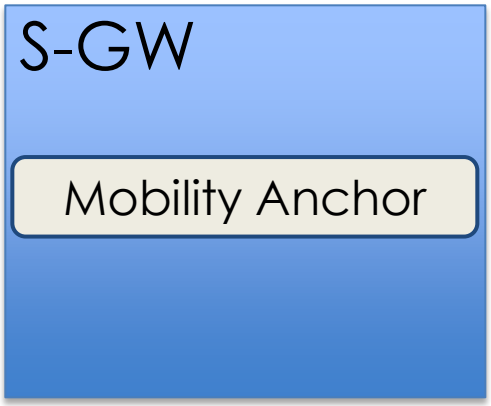
- **User equipment (UE)** – The LTE device
- **Evolved Node B (eNodeB or eNB)** – An evolved Node B (BTS)
- **E-UTRAN** - The radio network that exists between UEs and eNBs
- **Mobility Management Entity (MME)** – Primary signaling node (no user traffic). Large variation in functionality including managing/storing UE contexts, creating temporary IDs, sending pages, controlling authentication functions, and selecting the S-GW and P-GWs
- **Serving Gateway (S-GW)**- Carries user plane data, anchors UEs for intra-eNB handoffs, and routes information between the P-GW and the E-UTRAN
- **Packet Data Network Gateway (P-GW)** – Allocates IP addresses, routes packets, and interconnects with non 3GPP networks
- **Home Subscriber Server (HSS)** - This is the master database with the subscriber data
- **Authentication Center (AuC)** - Resides within the HSS, maps an IMSI to K, performs cryptographic calculations during AKA
- **IP Multimedia Subsystem (IMS)** – Paging, connections to the PSTN, and

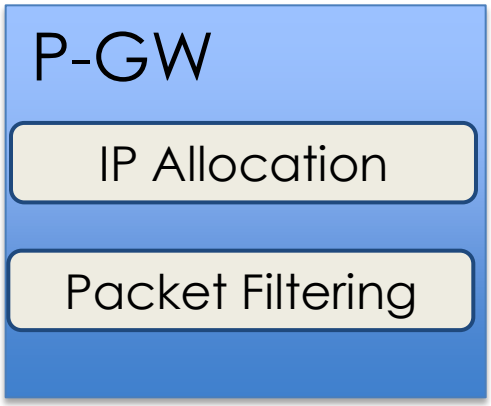
E-UTRAN & EPC Protocols



E-UTRAN







EPC

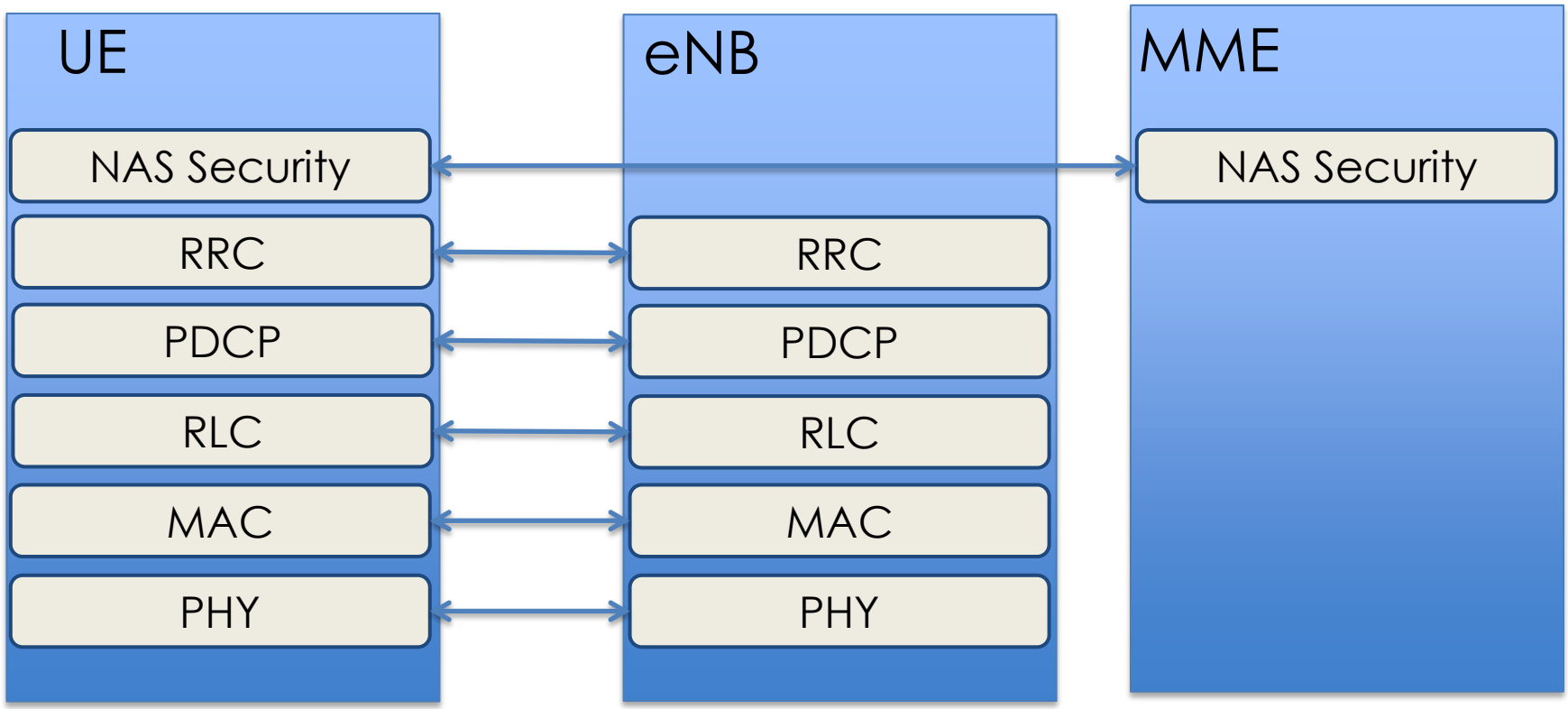
Green boxes depict the radio protocol layers. White boxes depict the functional entities of the control plane

Adapted from 3GPP TS 36.300

Protocol Discussion

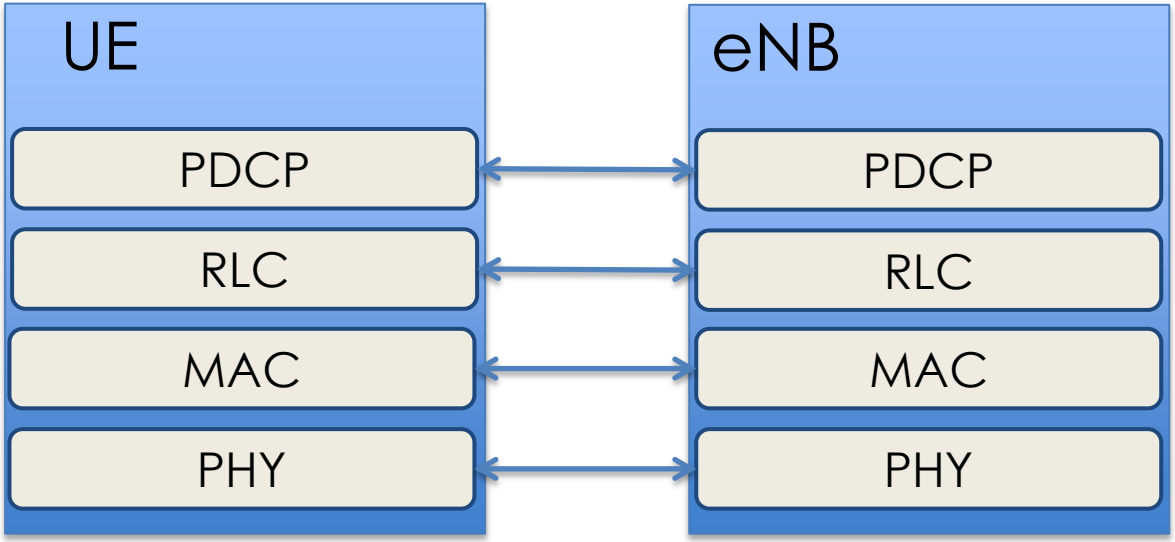
- There are a number of additional capabilities provided by the enB
  - IP header compression of user data stream
  - Selection of an MME at UE attachment when no routing to an MME can be determined from the information provided by the UE
  - Routing of User Plane data towards Serving Gateway
- **Radio 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

CP Protocols



Adapted from 3GPP TS 36.300

UP Protocols

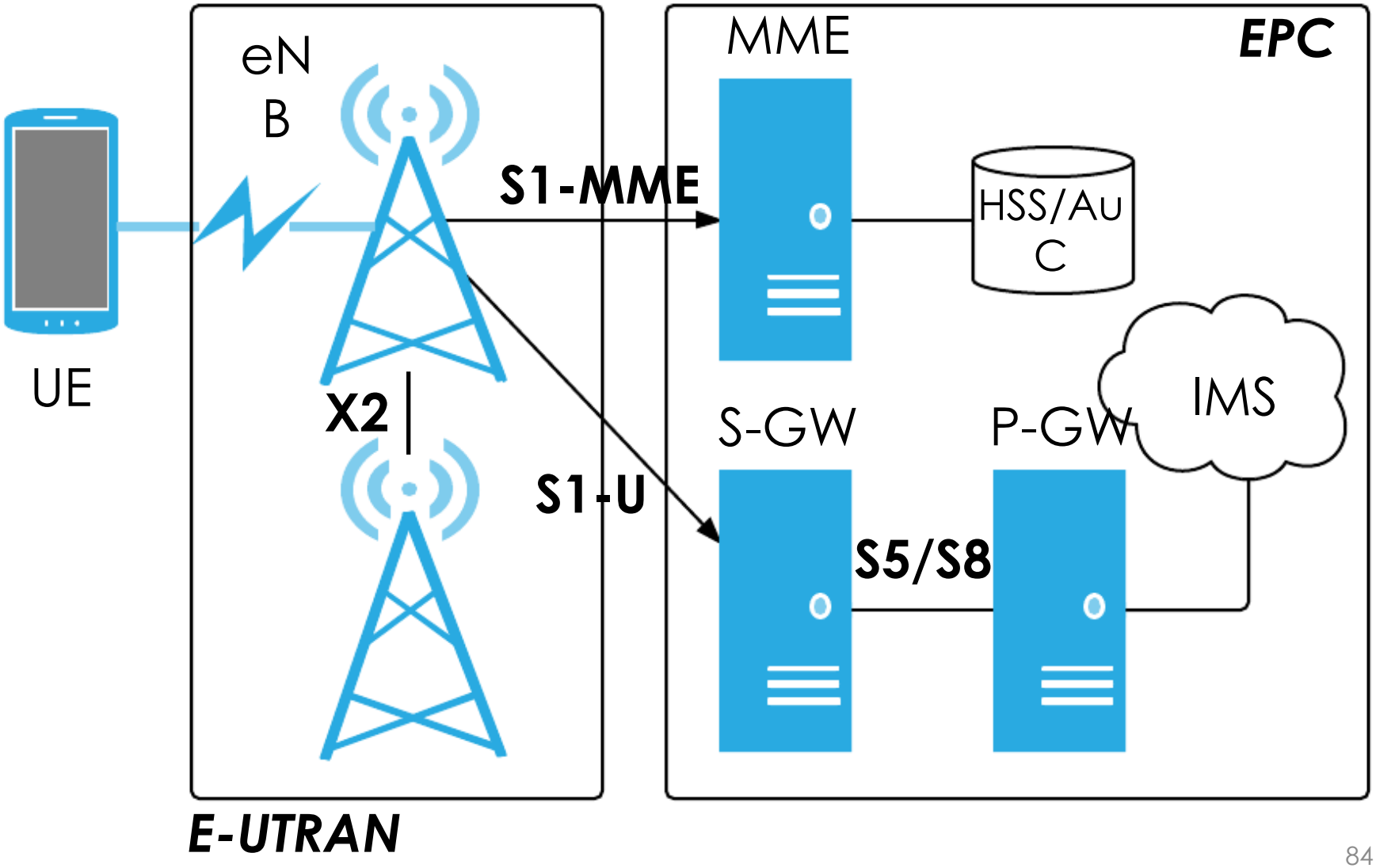


Adapted from 3GPP TS 36.300

Interfaces

- Interfaces are the communications paths LTE components use to communicate
- Each one is provided with its own label
  - There may be unique protocols between various interfaces
- There are many interfaces - we are discussing a subset
  - X2 - eNB to eNB
  - S1-U - eNB to S-GW
  - S1-MME (sometimes S1-C) - eNB to MME
  - S5/S8 - S-GW to P-GW

LTE/EPS Interface Diagram



LTE Security Mechanisms

- Continue to use the USIM hardware module
- Subscriber and network authentication via AKA
- Cryptography
  - Algorithms
  - Key hierarchy
  - Protected Interfaces
  - Protected Planes
- Independent Domains
  - Access Stratum (AS)
  - Non-access Stratum (NAS)

LTE Hardware Token

- The LTE USIM/UICC is identical to UMTS
- Contains a new hardware protected 128-bit key: K
  - As in GSM, never moves from UICC and HLR/AuC
  - Keys are derived from K as needed
  - AuC stores an IMSI and K

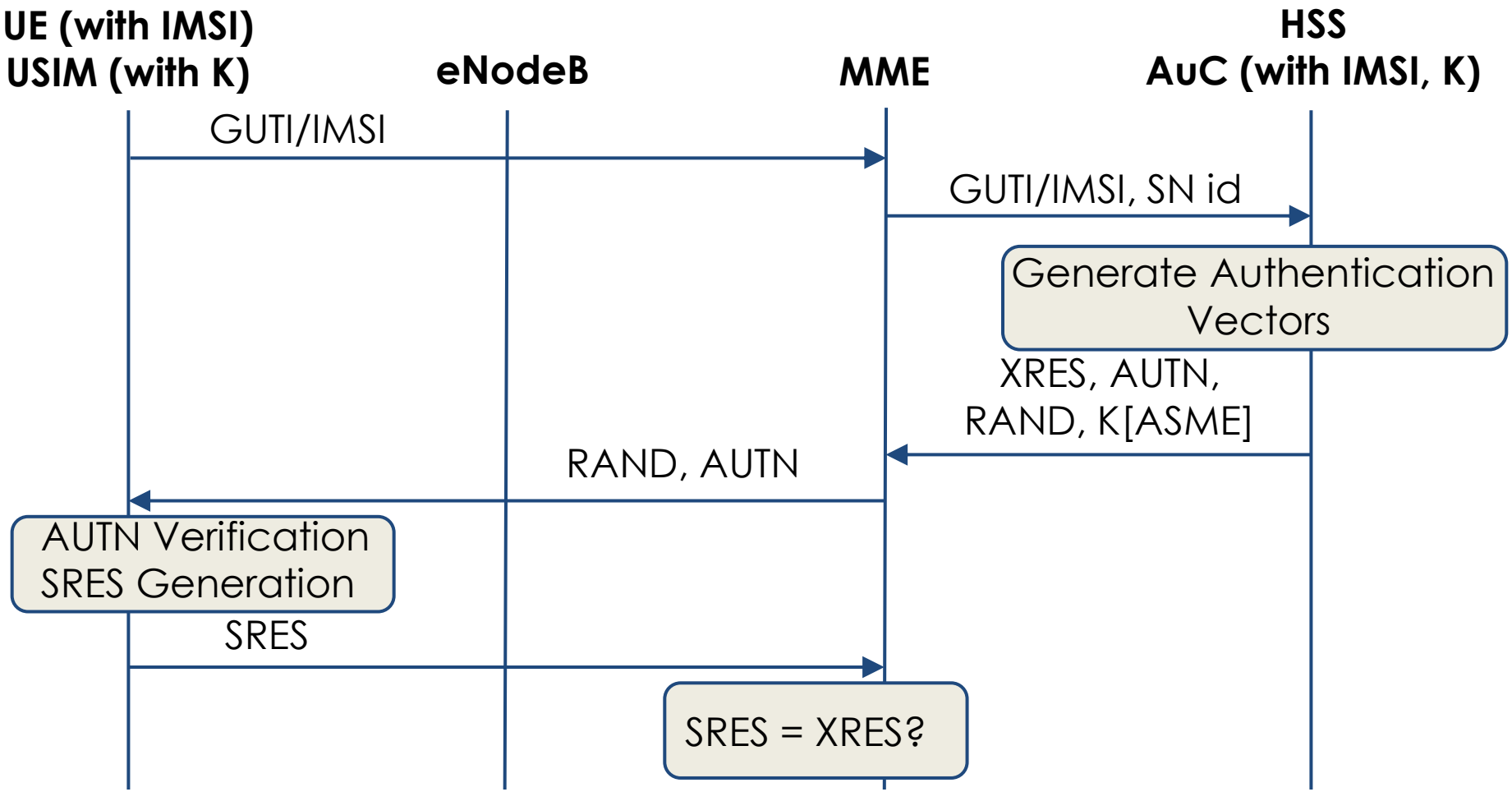
LTE AKA

- Very similar to GSM and UMTS AKA
  - Anchored in hardware token (UICC/USIM)
- 2G SIMs are deprecated
  - They are unable to authenticate to LTE
  - UEs may drop down to UMTS or GSM
- We will discuss LTE AKA in detail
  - Overall ladder diagram
  - Generation of AKA security parameters
  - Verification within the USIM

LTE AKA Discussion

- UMTS and LTE AKA are extremely similar
  - Originally specified in TS 33.102
  - So much so, the LTE standard doesn't even fully describe it (See TS 33.401)
- Largest update to AKA: network separation
  - Prevents a breach on one telco's network to spill into another's
  - Network identity is bound to certain keys
  - AKA directly authenticates network identity
- New key derivation function specified in LTE

LTE AKA Ladder Diagram



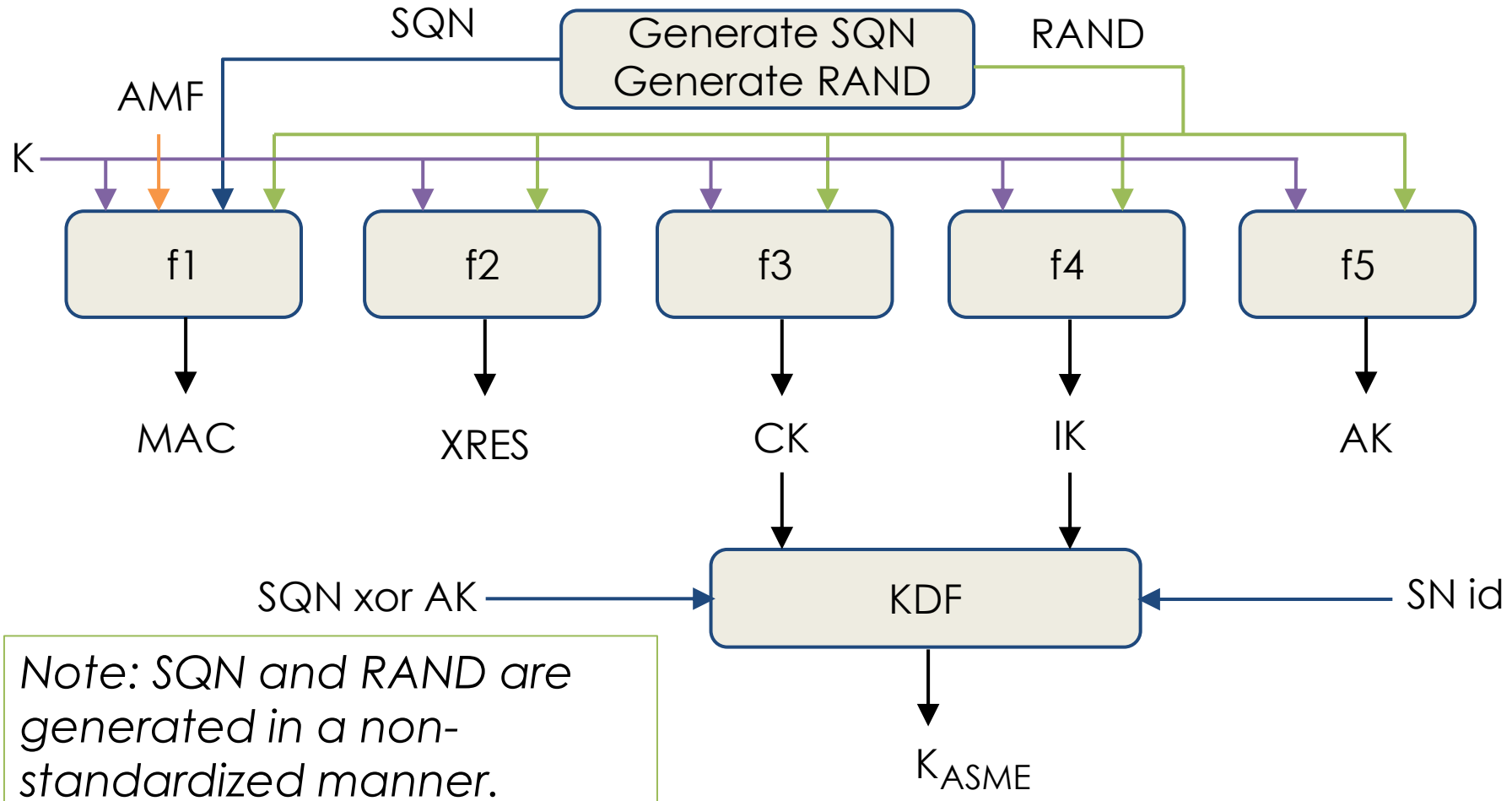
GUTI = Globally Unique Temporary Identity

Adatpted from 3GPP TS 33.102

AVs Generation

- The authentication vectors (AVs)are necessary to perform AKA
- They are requested by the MEE
  - Generated by the HSS/AuC
- LTE Authentication Vector = (XRES || AUTN || RAND || K[ASME])
- AK = Anonymity key
- AUTN = (SQN xor AK || AMF || MAC)
  - MAC = Message authenticate code in this instance
- AMF = Authentication Management Field
- CK = Cipher key
- IK = Integrity key
- KDF = Key derivation function
- MAC = A message authentication function
- SQN = Sequence Number
- XRES = Expected response
- SRES = Signed response

AVs Generation Diagram



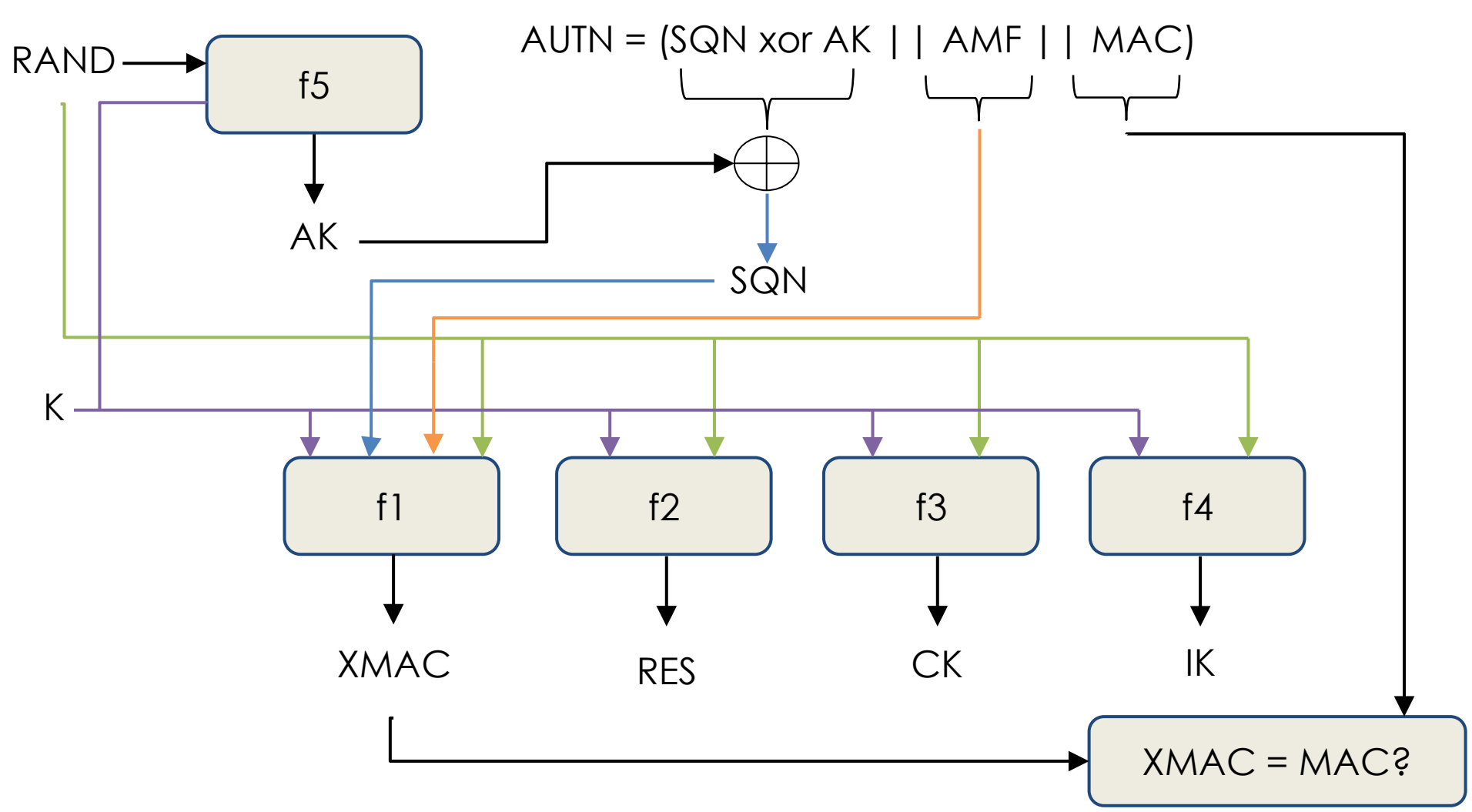
Note: SQN and RAND are generated in a non-standardized manner.

Adatpted from 3GPP TS 33.401

USIM Verification

- To verify the AVs in the USM, the authentication process is reversed
- The same functions f1 through f5 are implemented in the USIM
- If XMAC != MAC then an authentication failure occurs
  - There is a distinct process for this

USIM Verification Diagram

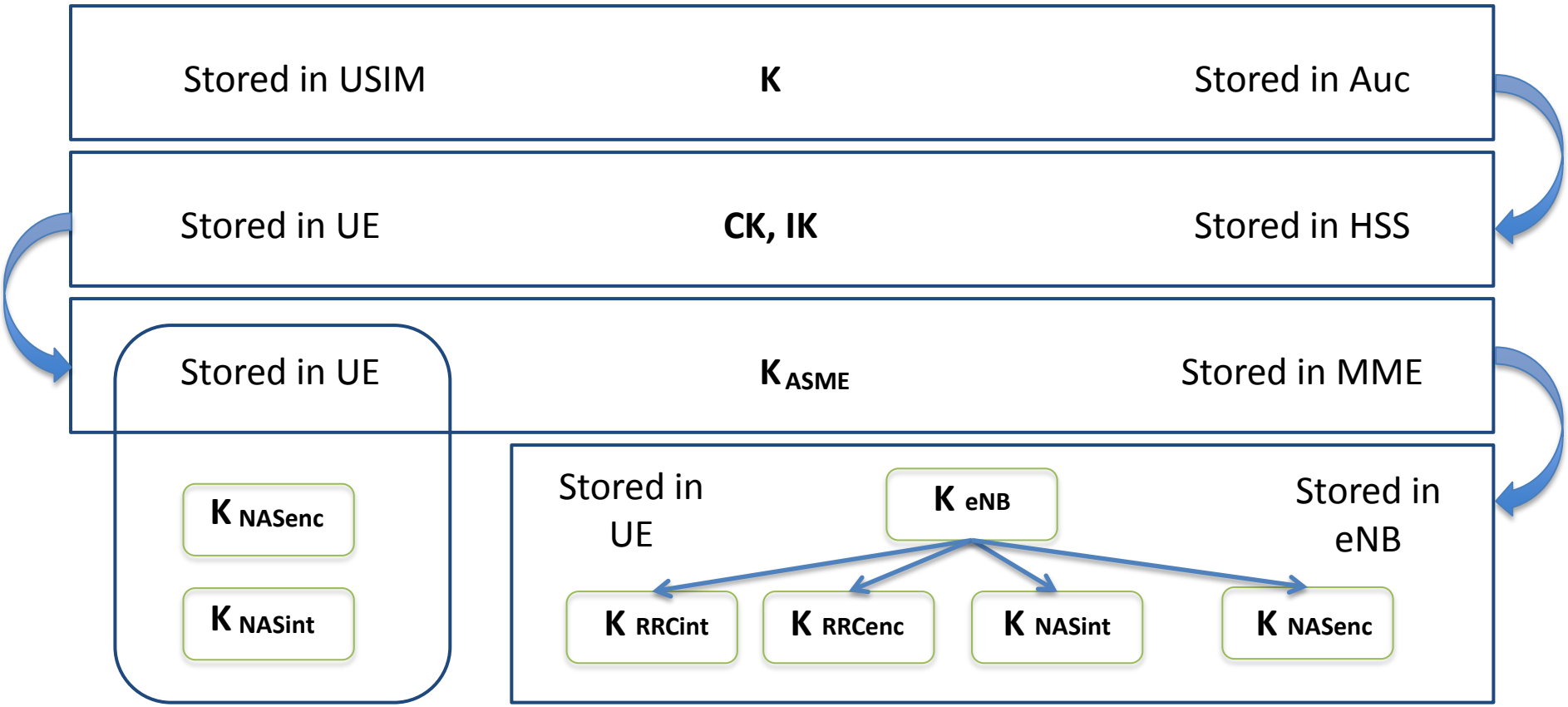


Adatpted from [3GPP TS 33.401]

Cryptography in LTE

- Large change to cryptographic key structure
  - Introduced a new set of intermediate keys
  - Unique keys for each connection/bearer - large complicated hierarchy
- Similar to UMTS, we have 2 sets of algorithms for confidentiality and integrity
  - EEA1/EIA1 - based on SNOW 3G
  - EEA2/EIA2 - based on AES (USA)
  - EEA3/EIA3 - based on ZUC (China)
- CP and UP may use different algorithms

Key Hierarchy



Adatpted from 3GPP TS 33.401

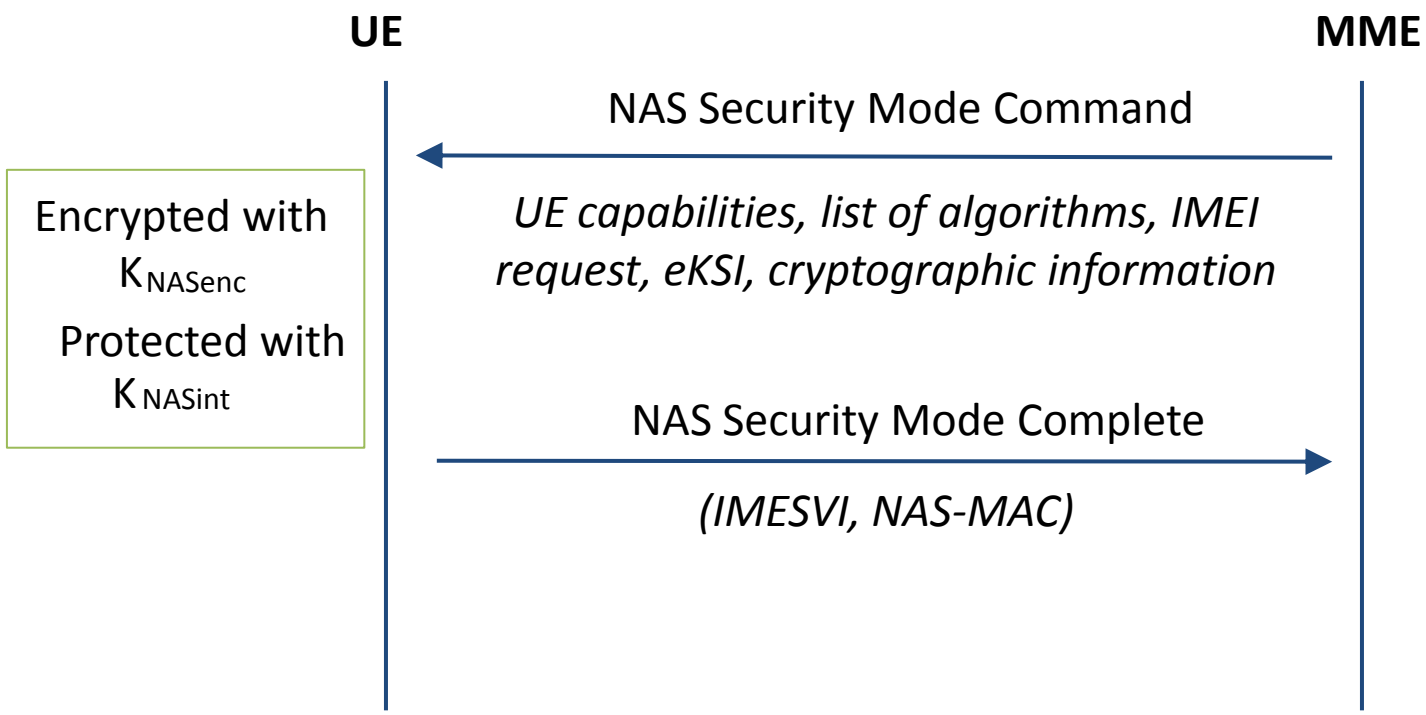
Key Discussion

- K – The master key. Permanent pre-shared key stored in hardware. Located on USIM and HSS/AuC
- CK and IK – Cipher key and Integrity key
- K[ASME] – Local master. The serving network ID (SNid) is used to derive this key in addition to CK and IK.
- K[eNB] – Used to derive additional keys used in handoff
- K[NASent] & K[NASint]- Protection of NAS traffic
- K[RRCent] & K[RRCint] - Protection of RRC traffic

LTE Non-Access Stratum

- Security-related signaling between UE and the backhaul
  - Algorithm selection occurs between the UE and the MME
  - MME contains a list of confidentiality and integrity algorithms in a priority order
- NAS negotiation precedes AKA
- Negotiation begins when an MME sends an integrity protected Security Mode Command to UE
  - Contains evolved key set identifier (eKSI), list of security capabilities and algorithms, IMSI request, and additional cryptographic information
- The UE responds with an integrity protected encrypted message called the NAS Security Mode Complete containing its IMEI and a MAC of the message

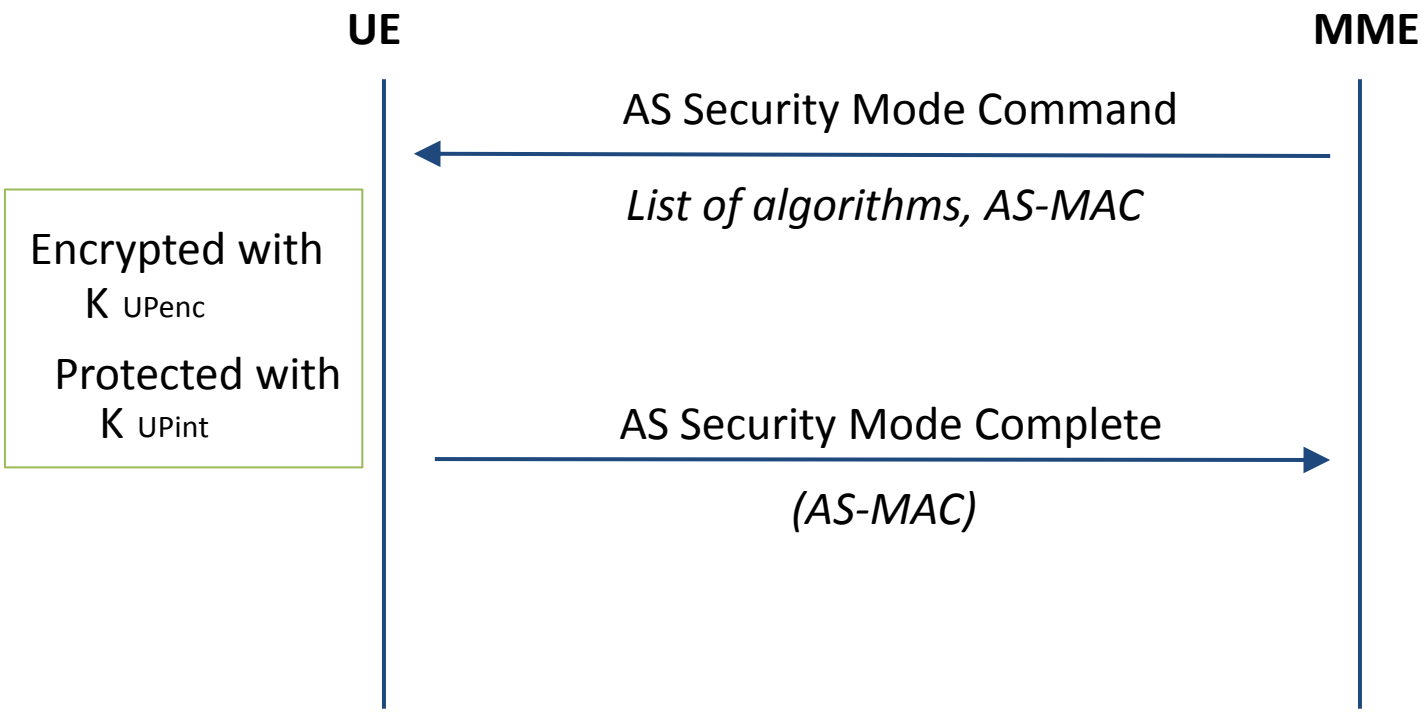
LTE NAS Negotiation



LTE Access Stratum

- Signaling between UE and eNB
  - Algorithm selection occurs between these components
  - eNB contains a list of confidentiality and integrity algorithms in a priority order
- AS and RRC communication occur on the Packet Data Convergence Protocol (PDCP)
- AS protection is optional

LTE AS Negotiation



Signaling Protection

- Network components create protected channels for each component that it is communicating with, for example:
  - UE and eNB communicate with a unique key
  - UE and MME communicate with a unique key
  - eNB and S-GW communicate with a unique key
- NAS security is always setup if a UE is registered to the network
- AS security is setup as needed
- A common claim is that LTE is "fully encrypted"
  - Initial radio access and signaling is not, but no data is being transmitted at that point
  - The standard states that ciphering may be provided to RRC-signaling
  - "RRC signaling confidentiality is an operator option."

Handover

- Unfortunately, UEs are constantly on the move
- This causes the need to be able to switch from eNB to eNB, and possibly from network to network
- The procedures for this are quite complex as keys and other protected information needs to be transferred or renegotiated
  - Cryptographic keys and encryption/integrity algorithms may need to be changed
  - Refer to our LTE Security book for additional details and the relevant 3GPP standard for additional information

Security Contexts

- Security contexts are a collection of security-related information
  - Algorithms, keys, and other parameters
- Many contexts are defined:
  - NAS and AS
  - Current and non-current
  - Native and mapped
- Depending on sensitivity they are stored in the USIM or the RAM of the UE

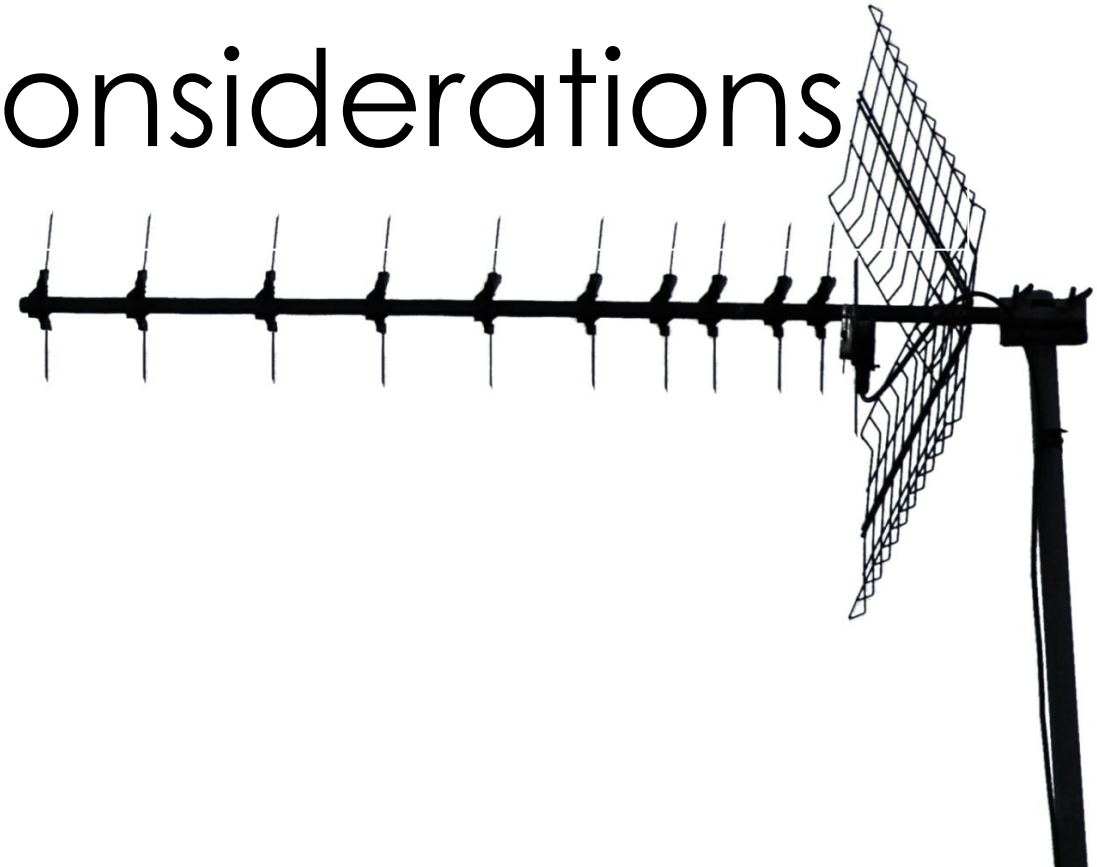
Backwards Compatibility

- At times LTE service may be lost and a 2G or 3G system may be available
- Security Contexts are mapped from one system to another
- A NAS security context is generated if moving to LTE
- K[ASME] is used to derive GSM/UMTS security contexts if needed
- Once mapping has occurred - a new native security context is reestablished as soon as possible
  - AKA can be run again as well

Lawful Interception

- Lawful interception mechanisms are built into 3GPP standards
- Call/message content and related data provided from certain network elements to the law enforcement side
- Assumes typically that the content appears in clear in the network element
- End-to-end encryption is still possible if keys are provided
- No weak algorithms introduced for LI purposes
  - All 3GPP algorithms are publicly known
- National variations exist
- Check TS 33.106, 33.107, and 33.108 more additional information

Research Considerations

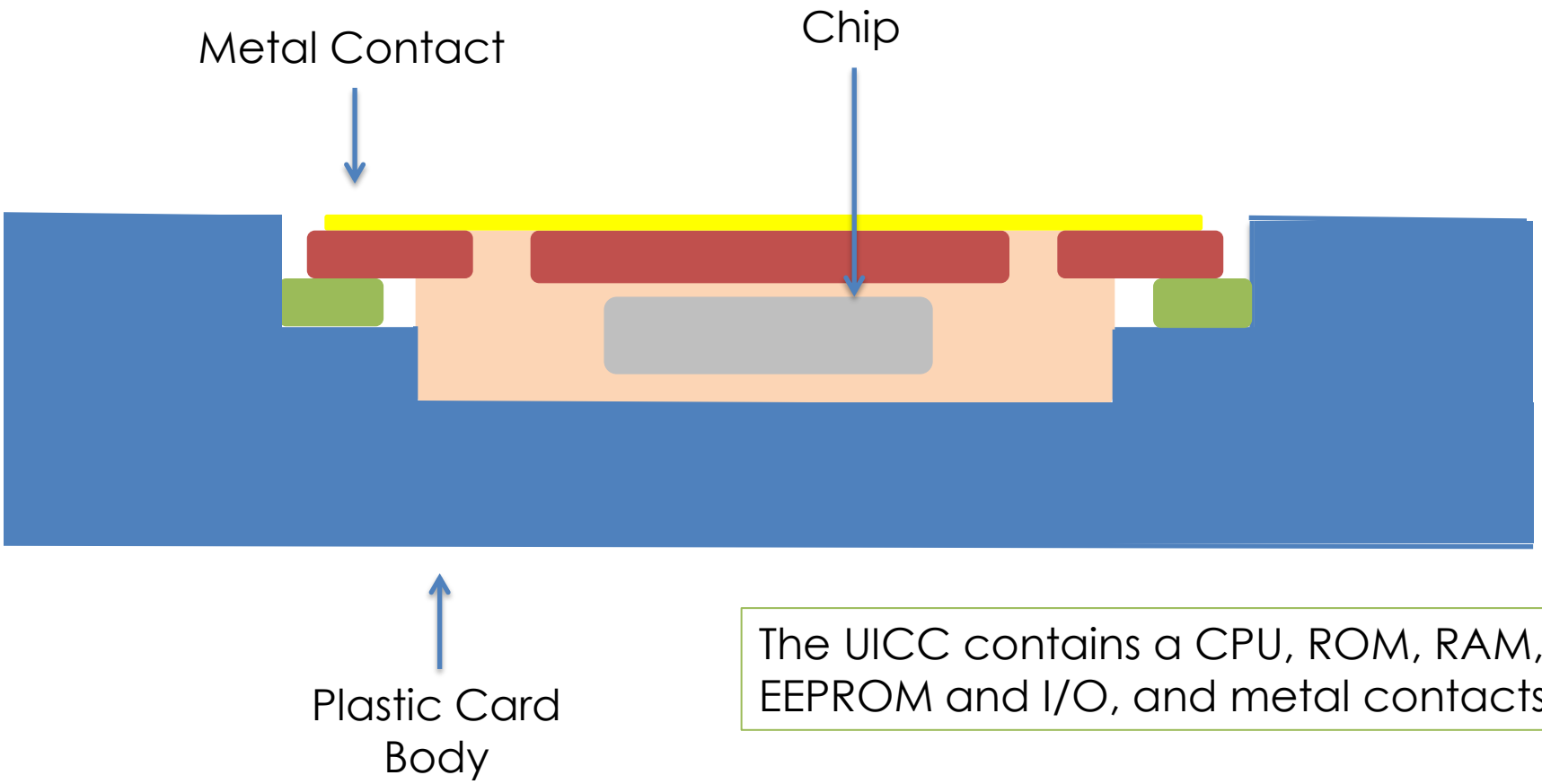


SIM Hacking

- SIMs can be locked using a PIN
  - PIN is required on phone reboot
  - If PIN is not provided a special code from the telco is required (Personal unlocking key = PUK)
- Stamped on most SIMs is the ICCID (Integrated Circuit Card Identifier
  - 18 digit unique identifier for the SIM
- SIMs are updated by over the air (OTA) text messages never displayed to a user
- Rooting SIM Cards, Blackhat 2013
- SIM Forensics
  - Exploring the OS of the SIM, looking for data

SIM Hacking

SIM Hacking



The UICC contains a CPU, ROM, RAM, EEPROM and I/O, and metal contacts.

Adopted from Anthony, Sebastian in references

Femtocells

- Often runs a Linux distro
  - To be used maliciously, root access is required
- Previous femtocell hacks exploit software vulnerabilities and factory reset procedures
- Phones automatically attach to the tower with the strongest signal, which is typically the closest tower
- IMSI-catcher – femtocell that is configured to look like a real base station to steal IMSIs from nearby devices
  - Often used by law enforcement
  - IMSIs are important for device/subscriber tracking and call interception
- Femtocells: A poisonous needle in the operator's hay stack, Borgaonkar et al at Blackhat 2011
- Traffic Interception & Remote Mobile Phone Cloning with a Compromised CDMA Femtocell, Doug DePerry et al Defcon 21

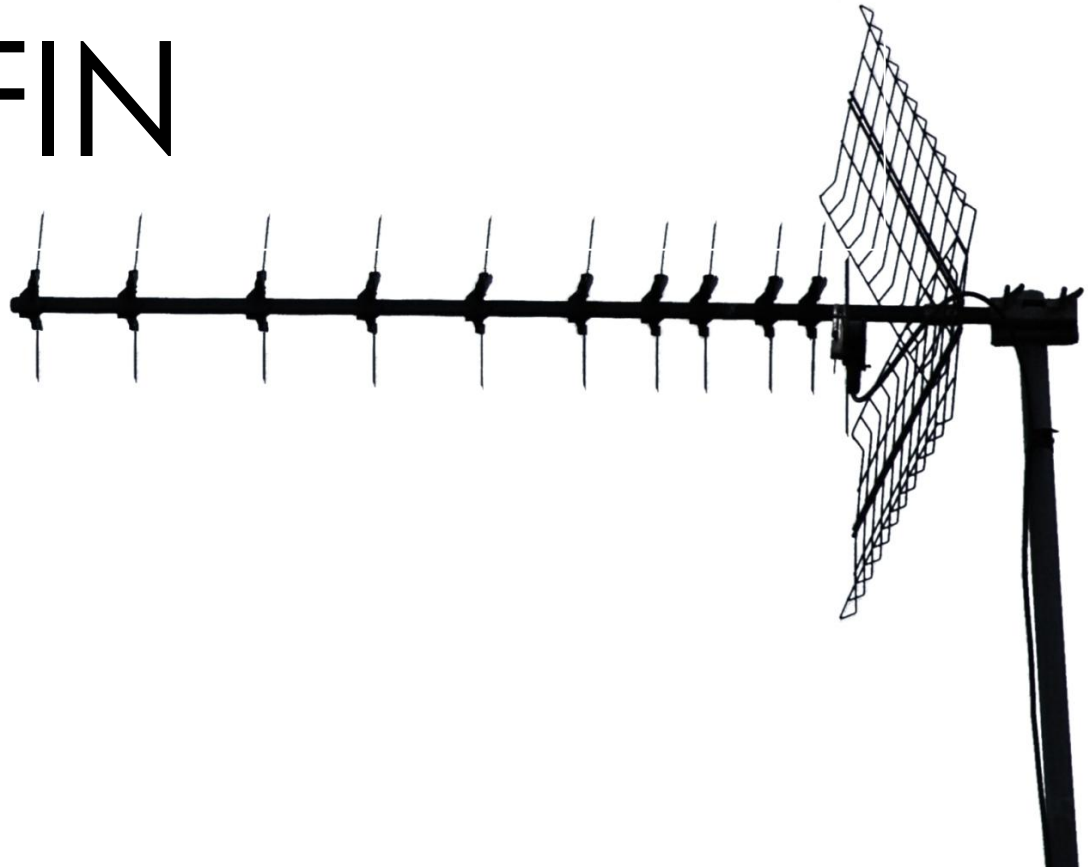
HeNB

- Home eNode Bs (HeNBs) connect to the backhaul via a distinct Security Gateway (SeGW)
  - Tunnel is protected with IPsec
- A hardware root of trust is included in modern HeNBs
  - Used to assist in secure boot and integrity check
  - Ensures that upon boot, key firmware and other sensitive security parameters are not modified
- The status of integrity checks are communicated to the SeGW

Baseband Hacking

- Going through baseband, one can attack the cellular software stack and the mobile operating system (i.e., Android, iOS)
  - Often leads to unlocking
- Some cellular stacks leverage legacy code
  - Often missing ASLR, NX, heap protection
  - Code not publicly available, reverse engineering of leaked binaries necessary
- Allows injection of packets via the air interface
- The IMEISV + IMEI often identifies the baseband software version
- You may need an external clock to assist with timing, as precision is required
- Notable work includes R.-P. Weinmann 2010, R.-P. Weignmann 2013 and Guillaume Delugre
- Femtocells: A poisonous needle in the operator's hay stack, Borgaonkar et al at Blackhat 2011
- Traffic Interception & Remote Mobile Phone Cloning with a Compromised CDMA Femtocell, Doug DePerry et al Defcon 21

FIN



In Conclusion

- More detailed security information can be found within:
  - *LTE Security* book,
  - 3GPP Standards (TS 33.401 especially), and
  - Various presentations and whitepapers throughout the web:
    - *Security Investigation in 4G LTE Wireless Networks*
    - Technical Overview of 3GPP LTE
- There's a lot more to cellular security than what is contained within this presentation
  - Study up!

Questions | | Thoughts?

- I want this presentation to be accurate
  - Please report errors and omissions (acknowledgement will be provided)
- Many links went dark while developing this presentation
  - External documents and references (other than videos) are also hosted on my personal domain to ensure they live on
  - All links are properly referenced in the final slide
- *Cellular Security - Part 2* will include a much deeper analysis of LTE networking protocols, crypto, IMS, handover, network interconnection, SIM forensics, and SIM/baseband hacking
  - And other requested topics

Joshua Franklin
www.jfranklin.me
josh dot michael dot franklin at gmail


– @thejoshpit

Resources & References

- [Hulton08] Hulton, Steve, Intercepting GSM Traffic, Black Hat 2008.
- Paget, Practical Cellphone Spying, Defcon 2010.
- Nohl, Karsten, Attacking phone privacy, Blackhat 2010.
- [Borgaonkar11] Borgaonkar, Nico, Redon, Femtocells: a Poisonous Needle in the Operator's Hay Stack.
- [Perez11] Perez, Pico, A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications, Black Hat DC 2011.
- [Nyberg04] Cryptographic Algorithms for UMTS
- *Dr. Maode Ma, Security Investigation in 4G LTE Wireless Networks*
- *Muyung, A Technical Overview of 3GPP LTE*
- Agilent, LTE and the Evolution to 4G Wireless: Bonus Material: Security in the LTE-SAE Network, Agilent
- Anthony, Sebastian, The humble SIM card has finally been hacked: Billions of phones at risk of data theft, premium rate scams
- Nohl, Karsten, Rooting SIM Cards, Black Hat 2013
- Weinmann, R., The Baseband Apocalypse
- Weinmann, R., Baseband Exploitation in 2013
- Guillaume Delugre, Reverse engineering a Qualcomm baseband
- TS 33.401 – LTE Security Architecture
- TS 33.102 - 3G security; Security architecture
- TS 36.300 – Overall description of E-UTRAN

Errors and Omissions

- Thanks to all that helped make this possible by providing feedback and identifying errors and omissions:

Tomasz Miklas
ph0n3lx
Skrattar
Baddkrash
Netsecluke
Nechered
Chloeeeeeeeee
Dr. Kerry McKay
BuildTheRobots