MACIEJ MAZUR

INTRO TO MOBILE NETWORK SECURITY

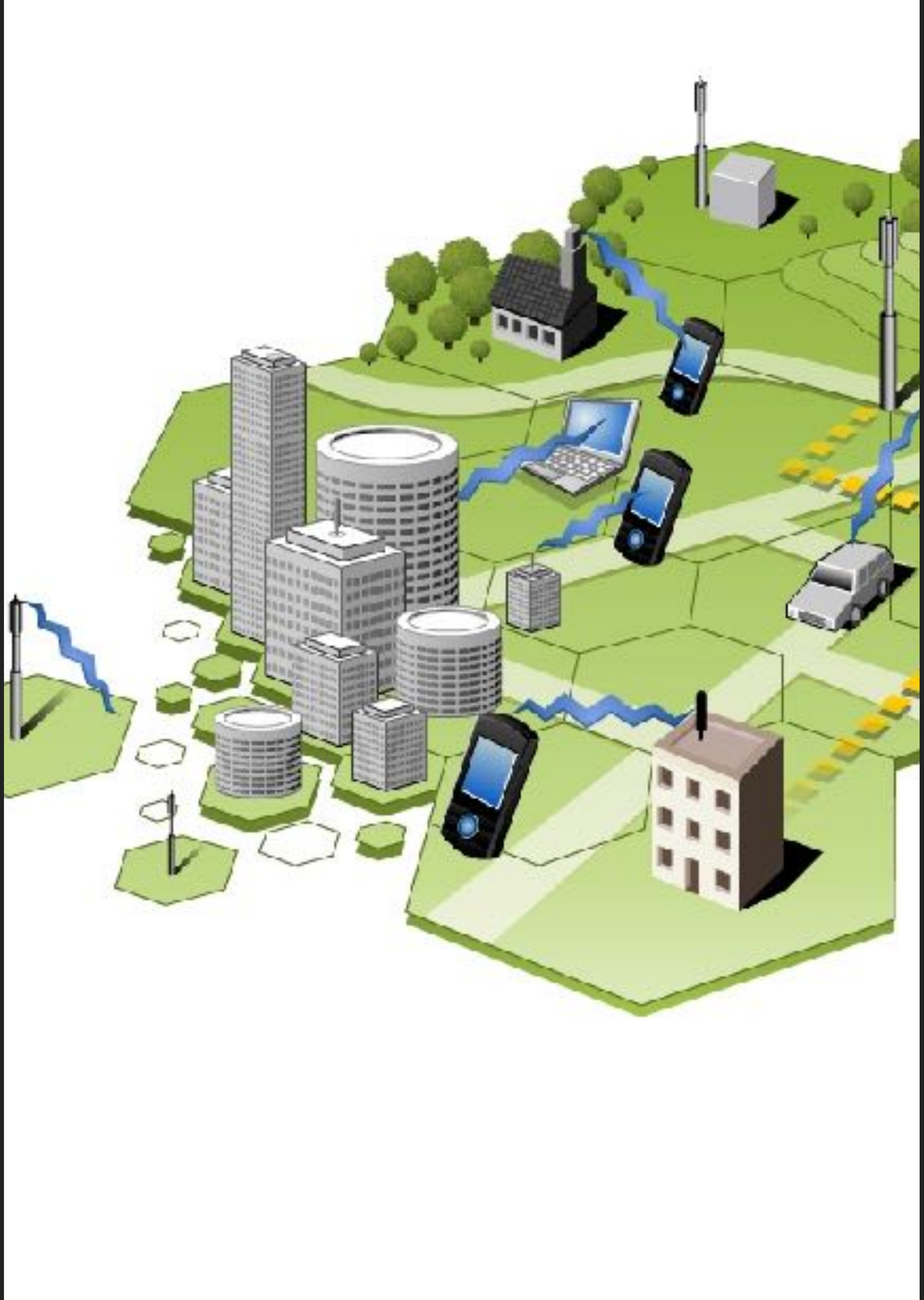
WHO AM I

- 10 years in telco
- worked with both radio (all generations) and core for vendors and MNO’s
- currently Solutions Architect in HPE CSB
- working in data science, security is just a hobby
- Opinions expressed are solely my own and do not express the views or opinions of my dog, lawyer and especially my employer
- all of the examples are given for educational purposes, before doing any “research” talk with your lawyer ;)

BASICS OF MOBILE NETWORKS SECURITY

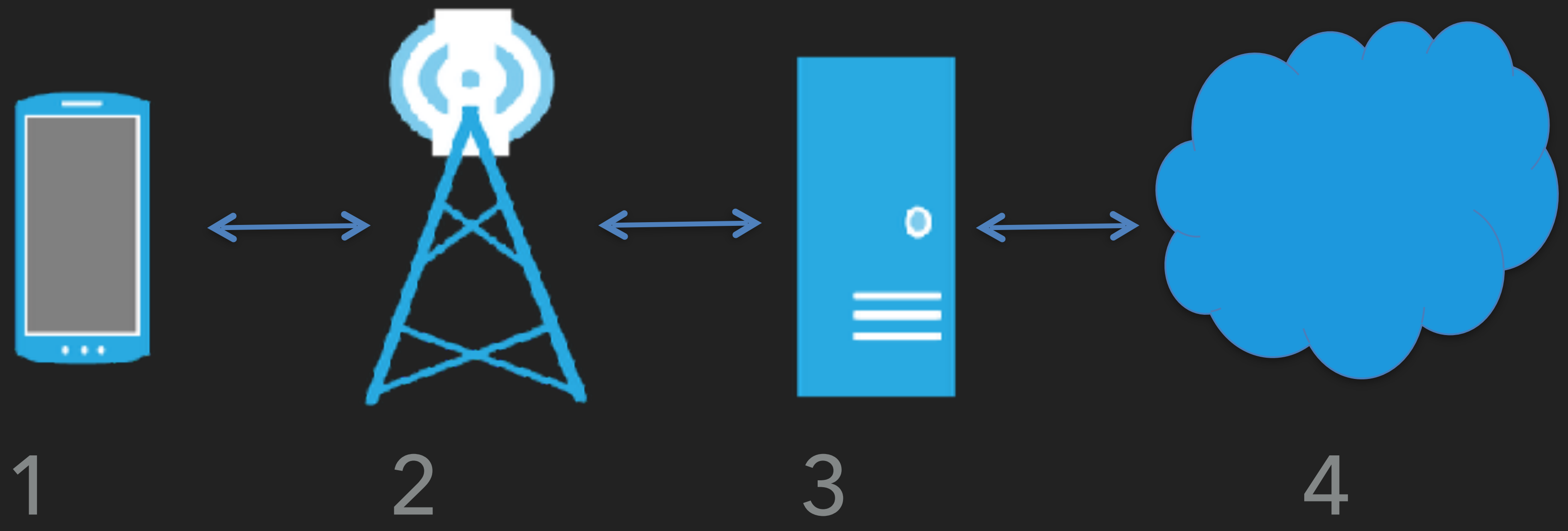
CELLULAR NETWORKS

- complex and interconnected
- 5+ billions of subscribers worldwide
- provides many services (voice, video, data, payments, location …)
- standards are large and complicated
- many competing standardisation bodies



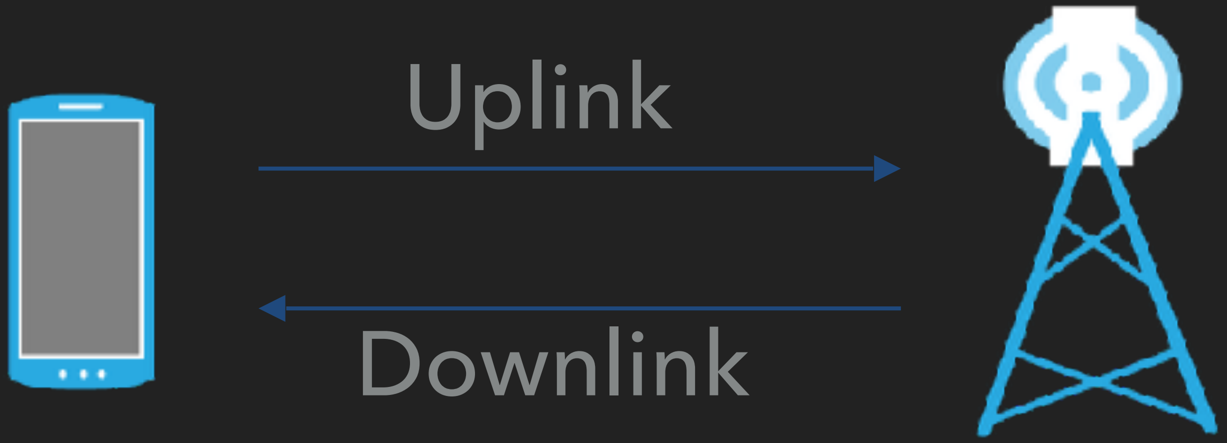
OVERVIEW

- UE (user equipment) is connect to a base station which connects to a backhaul network, which connects to the internet.



UPLINK AND DOWNLINK

- 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



FREQUENCIES

UNITED
STATES
FREQUENCY
ALLOCATIONS
THE RADIO SPECTRUM
RADIO SERVICES COLOR LEGEND
ACTIVITY CODE
ALLOCATION USAGE DESIGNATION
0 kHz
300 kHz
300 kHz
3 MHz
3 MHz
30 MHz
30 MHz
300 MHz
300 MHz
3 GHz
3 GHz
30 GHz
NOT ALLOCATED
RADIONAVIGATION
MARITIME MOBILE
FIXED
BROADCASTING
RADIONAVIGATION

RF 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

ANTENNAS

- 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

UE ANTENNAS

- 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), can be MIMO (multiple antennas)
  - WiFi (Primarily 2.4 GHz, 5 GHz) [there are other odd frequencies specified]
  - Bluetooth (2400–2480 MHz)
  - NFC (13.56 MHz)
  - GPS, GLONASS …

UE

- These are the devices with wireless radios that connect to cell towers. Radios are inside phones, tablets, laptops, etc. . .
- 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, rom companies like Qualcom
- 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) for performance reasons
- Sometimes shares RAM with application processor :)
- In a shared configuration the baseband is often the master
- May be virtualised

COMMUNICATION PLANES

- 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
- 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) singling
  - Voice and data information

PACKET AND CIRCUIT SWITCHING

- Pre-LTE, cellular networks used circuit switching technology for voice
- LTE uses VoLTE which is VoIP (like Skype) over LTE
- 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

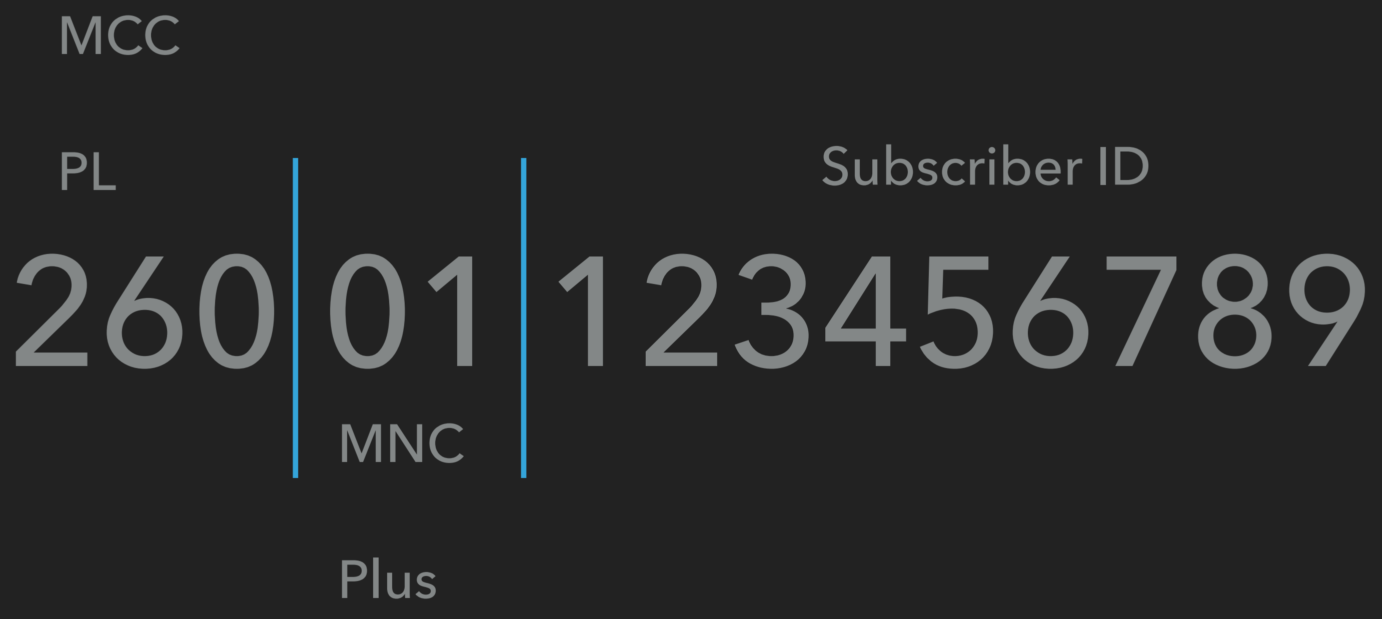
ATTACH, HANDOVER, PAGING

- 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 a call will need to be transferred from one base station to another
  - This is called handover
  - 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

SUBSCRIBER

- 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
    - 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



MCC

PL

Subscriber ID

260 | 01 | 123456789

MNC

Plus

IMEI

- GSM, UMTS, and LTE all contain a unique ID for a 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 CARD

- A removable hardware token used for GSM, UMTS, and LTE
  - eSIM coming now which will be embedded into device
- Over 8 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 SMS 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

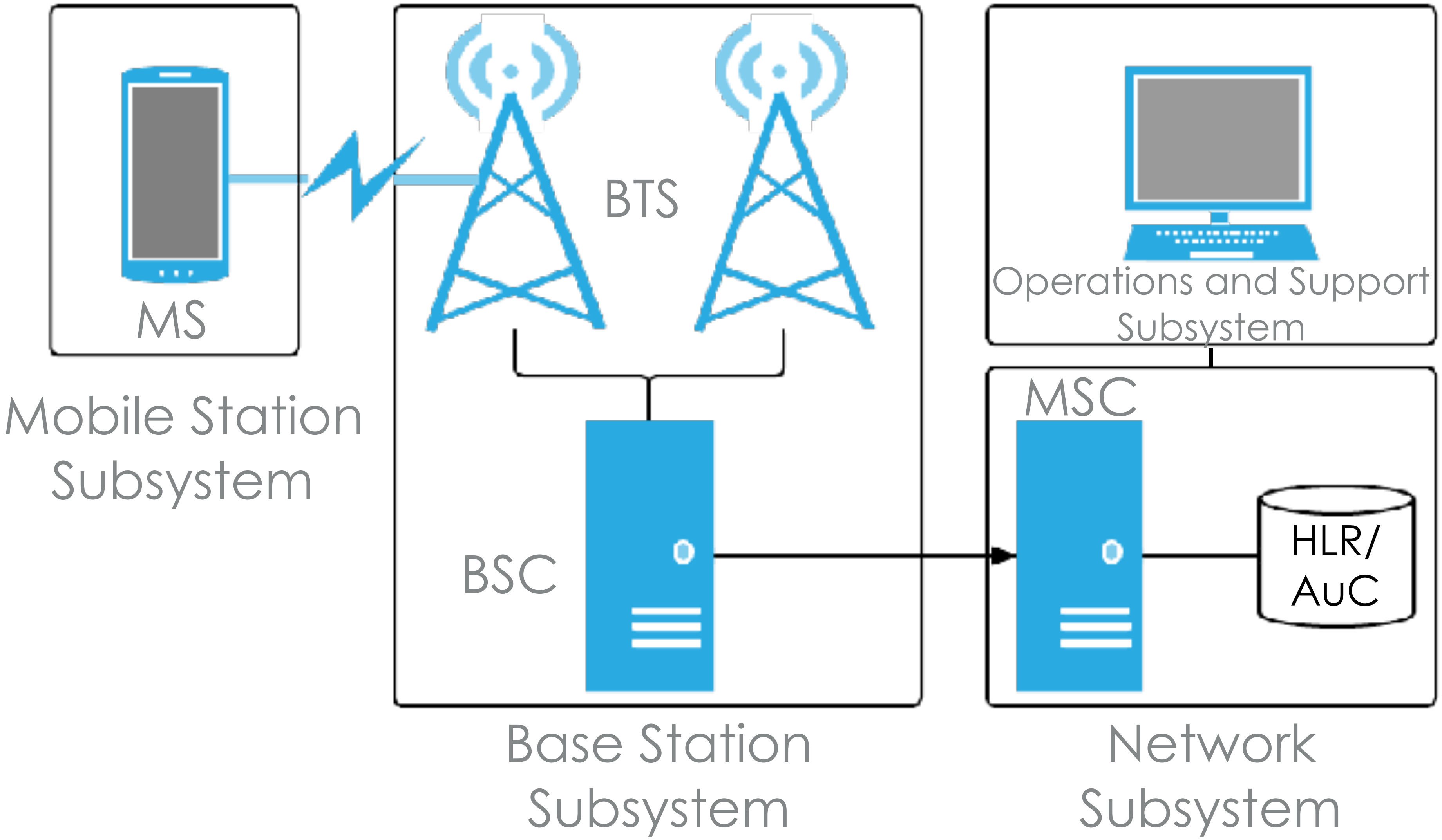
GSM – 2G

- 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 – COMPONENTS

- 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 SCHEMATICS



GSM SECURITY

- 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

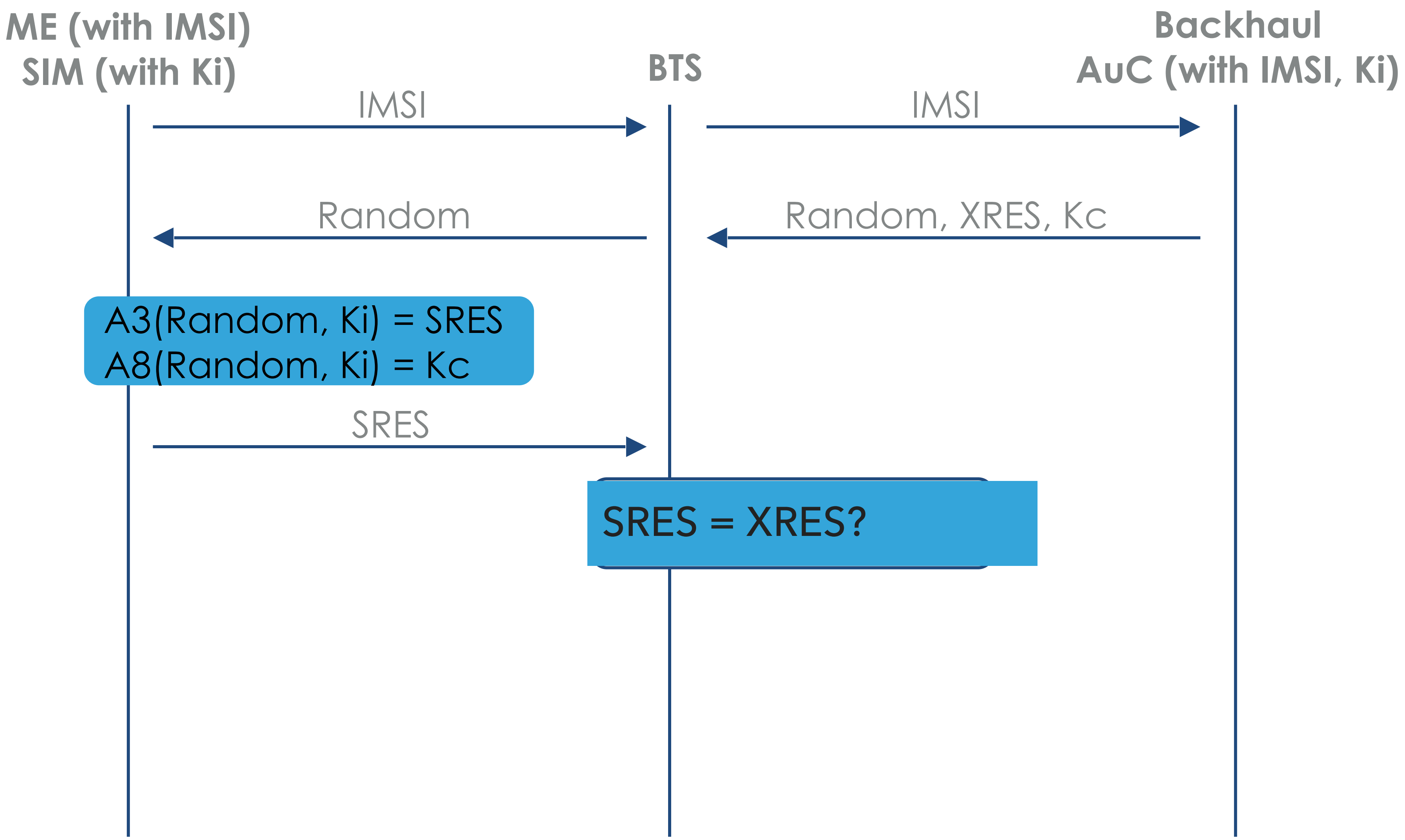
GSM SIM

- 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


ME (with IMSI)
SIM (with Ki)
BTS
Backhaul
AuC (with IMSI, Ki)
IMSI
IMSI
Random
Random, XRES, Kc
A3(Random, Ki) = SRES
A8(Random, Ki) = Kc
SRES
SRES = XRES?

GSM THREATS

- 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

GSM MOST NOTABLE ATTACKS

- Hulton, 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

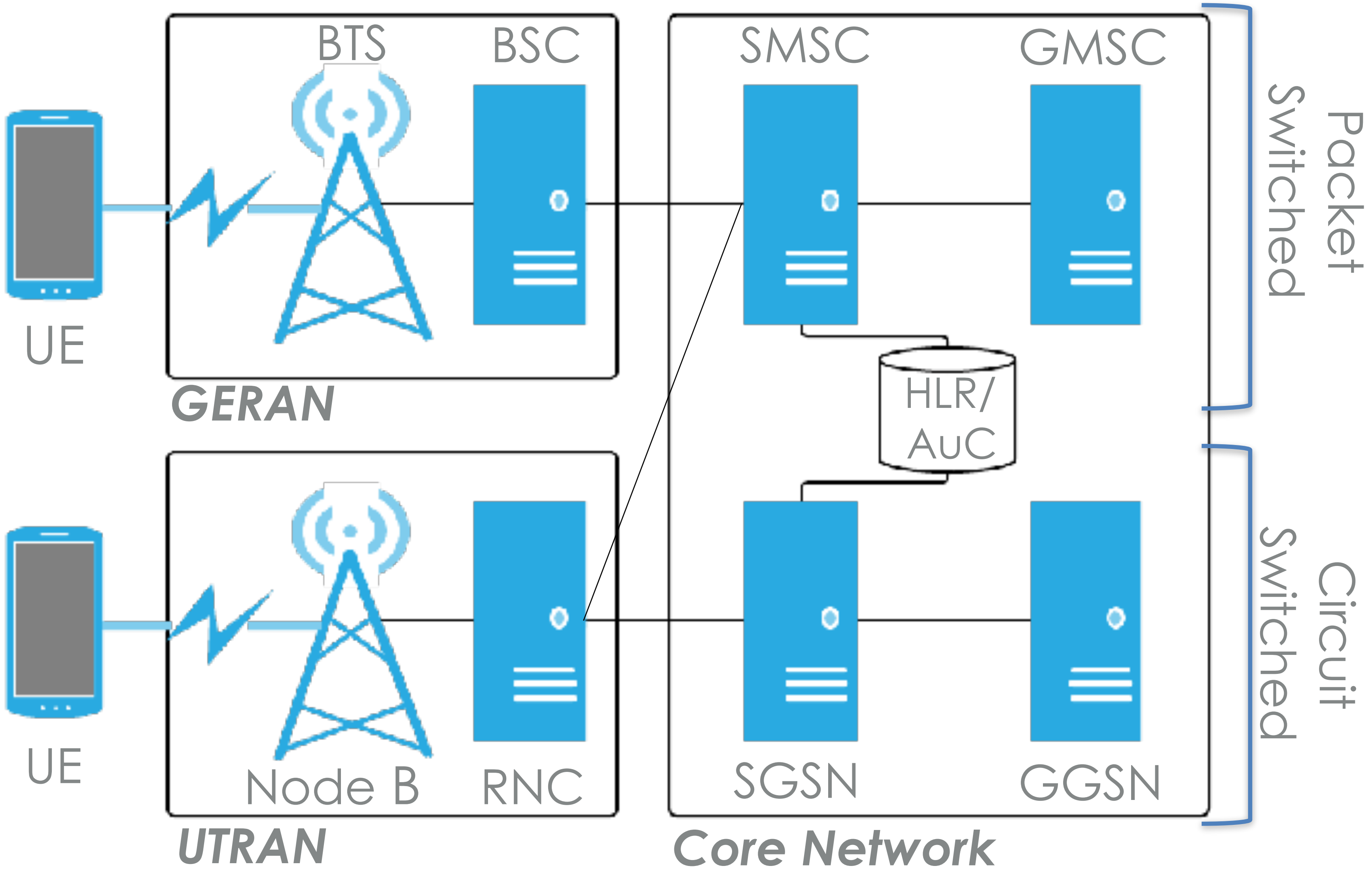
UMTS

- 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)
- There are many more network elements but this is an introduction

UMTS DIAGRAM



UMTS SECURITY

- 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 HW 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

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

- 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 in most networks falls back to older networks for voice (Circuit-switched fallback)
- VoLTE (voice over LTE)

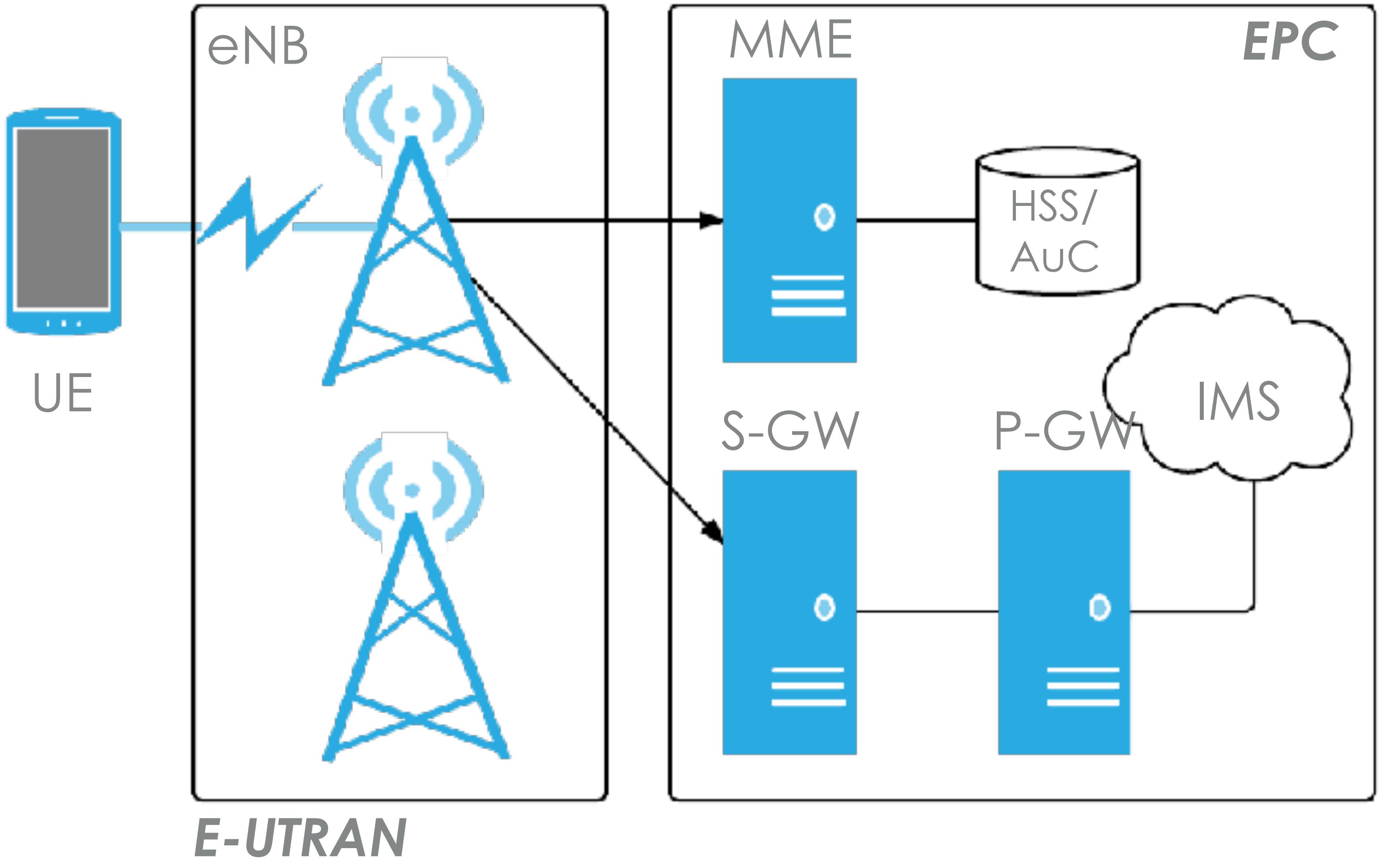
LTE THREATS

- 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
- Lawful interception - in theory it's a feature not a threat

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 DIAGRAM



LTE COMPONENTS

- 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)

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) - UE to eNB
  - Non-access Stratum (NAS) - UE to backhaul

LTE HW 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

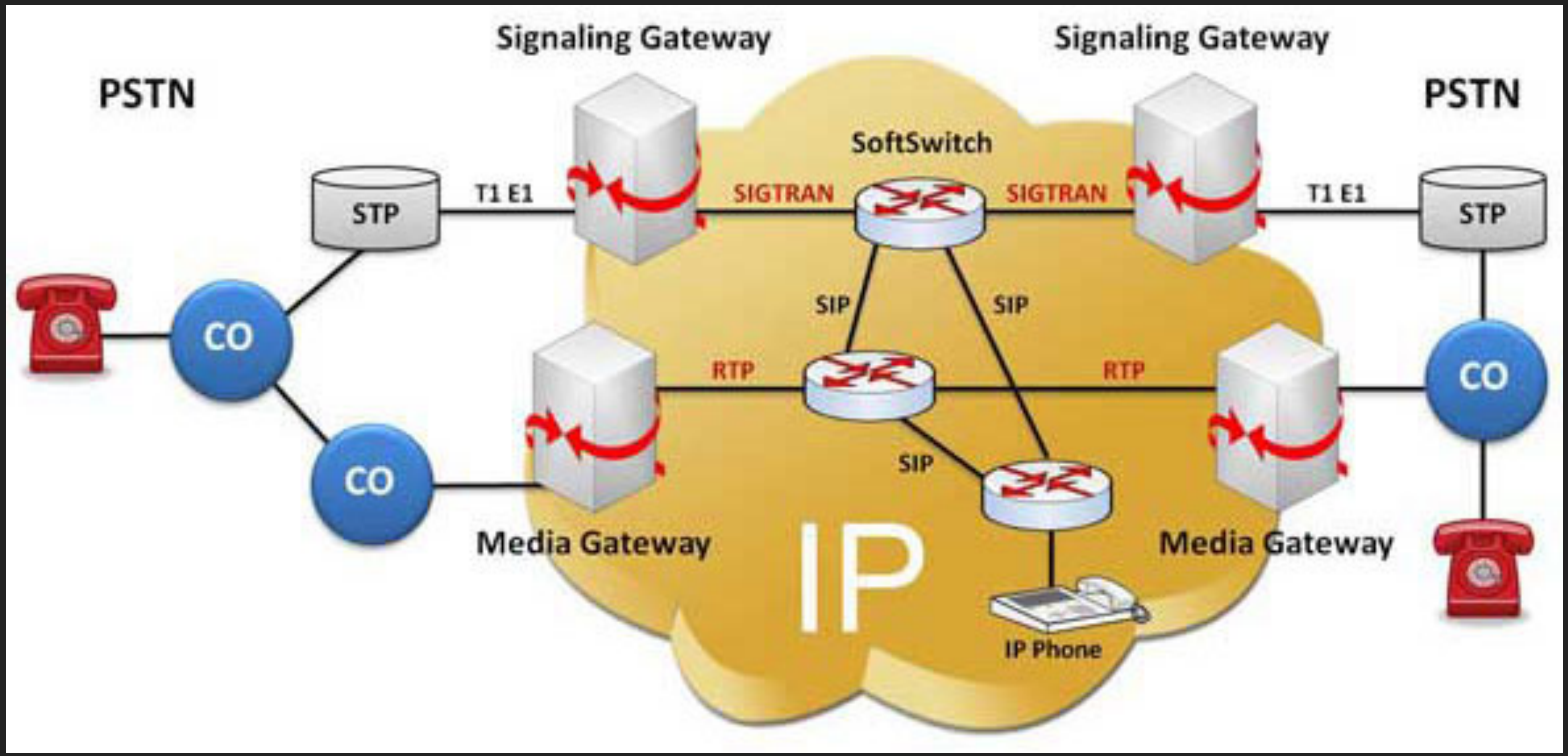
LAWFUL INTERCEPTION

- 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

SS7

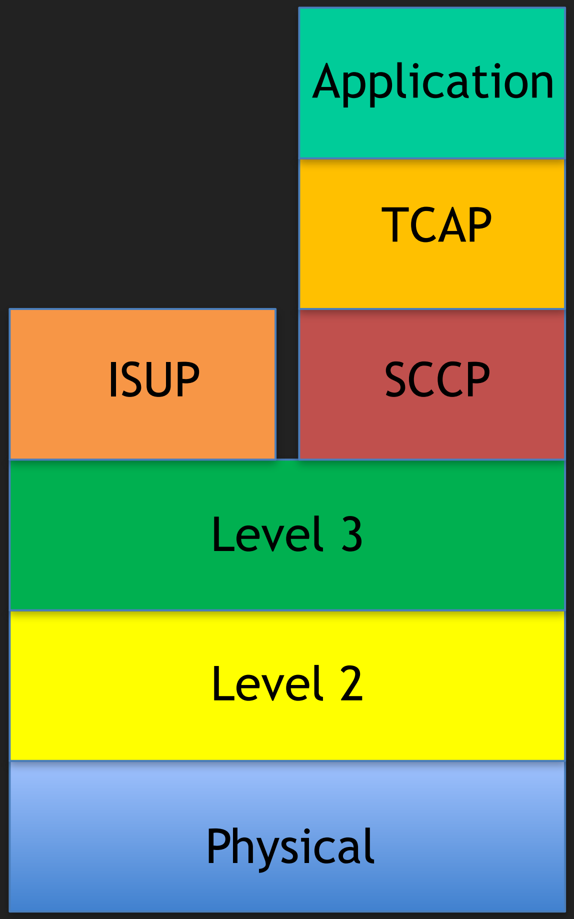
- Mobile networks primarily use Signalling System no. 7 (SS7) for communication between networks for such activities as authentication, location update, and supplementary services and call control. The messages unique to mobile communications are MAP messages.
- The security of the global SS7 network as a transport system for signalling messages e.g. authentication and supplementary services such as call forwarding does not exist.
- The problem with the current SS7 system is that messages can be altered, injected or deleted into the global SS7 networks in an uncontrolled manner
- Your SMS messages can be read because of this (banking, two factor authentication), your calls may be forwarded (to the recording machine and then to your friend you are calling), your location is compromised

SS7


Signaling Gateway
Signaling Gateway
PSTN
PSTN
SoftSwitch
STP
T1 E1
SIGTRAN
SIGTRAN
T1 E1
STP
CO
SIP
SIP
RTP
RTP
CO
CO
SIP
Media Gateway
IP
Media Gateway
IP Phone

SS7

The SS7 stack



SS7

- Mobile network uses SS7 signalling for call control, mobility management, short messages and value-added services
- MTP1-3: Message Transfer Part
- SCCP: Signalling Connection Control Part
- TCAP: Transaction Capabilities Application Part
- MAP: Mobile Application Part
- BSSAP: Base Station Subsystem Application Part
- INAP: Intelligent Network Application Part
- CAMEL: Customised Application for Mobile Enhanced Logic

SS7

- In the past, SS7 traffic was passed between major MNO’s
- Now many small operators and MVNO’s enter the market
- Many protocol converters for SS7 data to IP, primarily for voice and data over the IP networks as part of IN
- cheap PC based equipment can be used to access networks and the ready availability of access gateways on the Internet = lead to compromise of SS7 signalling

SS7 – HOW MNO’S TRY TO MAKE THE SITUATION BETTER

- SS7 traffic filtering and monitoring
- agreements with roaming partners and carrying out roaming testing, review of messages and also to seek appropriate confirmation that network operators are also screening incoming SS7 messages their networks to ensure that no rogue messages appear

SUMMARY

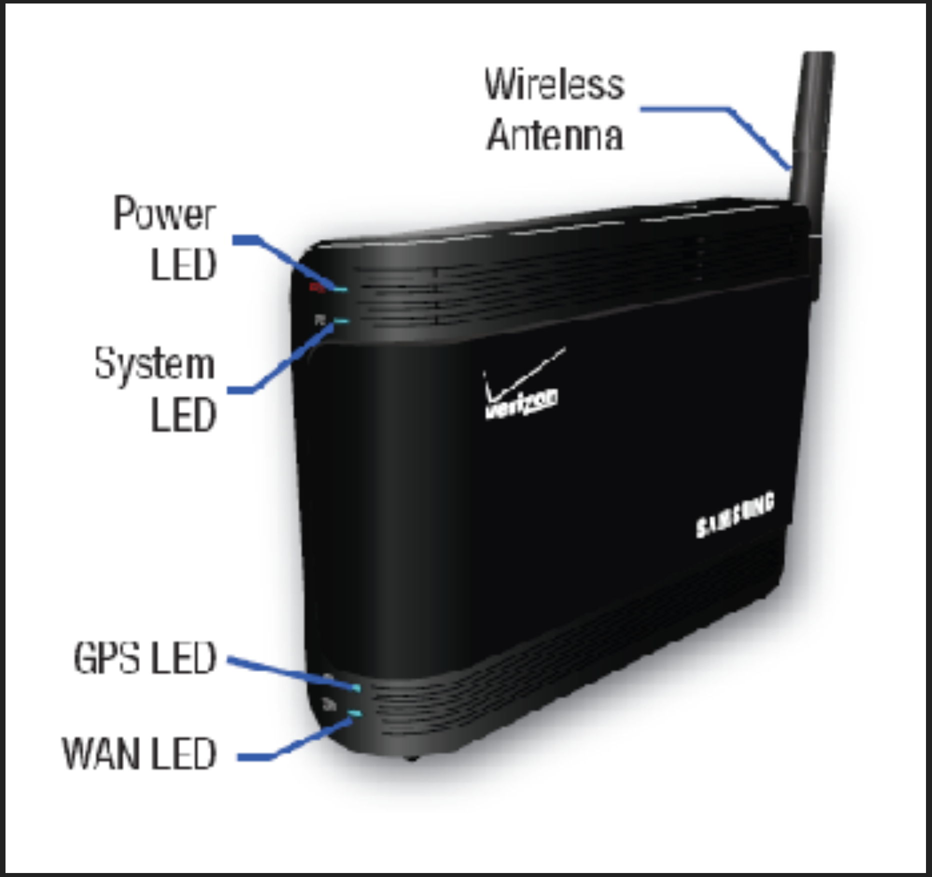
MOST COMMON THREATS TO MOBILE NETWORKS

- Charging fraud, unauthorised use
- Charging disputes
- Handset cloning (impersonation attack)
  - multiple handsets on one subscription
  - let someone else pay for your calls
- Voice interception - casual eavesdropping and industrial espionage
- Location tracking
- Call and location data retention
- Handset theft
- Handset unlocking (locked to a specific operator)
- Network service disruption (DoS)
- What about integrity?

BIGGEST PROBLEMS IMO

- security is not a first class citizen, MNO’s are maximising ARPU (average revenue per user)
- security based on “secret internal knowledge”, old protocols did not consider security as an issue
- many contradicting standards, and vendors which never implement a standard in 100%
- backwards compatibility
- current NFV movement and connecting telco world with IP networks opens everything to new attack vectors
- unrealistic assumptions (physically protected channels don’t need encryption)

PHYSICALLY PROTECTED ?



HOW TO START WITH MN SECURITY

BOOKS

- Wireles Crash Course - Paul Bedell
- LTE Security - Wiley
- LTE-Advanced for Mobile Broadband - Eric Dalhman

TOOLS AND OPEN SOURCE PROJECTS - CORE

- Linux (basic CLI tools)
- Wireshark
- SIPP
- http://www.openimscore.com
- https://github.com/openss7/openss7
- https://www.onap.org

TOOLS AND OPEN SOURCE PROJECTS - RADIO

- Wireshark
- http://openbts.org
- https://github.com/srsLTE/srsLTE
- https://sourceforge.net/p/openlte/wiki/Home/
- HackRF or similar from Aliexpress

LICENSE

based on materials authored by Joshua Franklin

Q&A