DEPARTMENT OF
COMPUTER
SCIENCE

UNIVERSITY OF
OXFORD

Authentication and related threats in 2G/3G/4G networks

Ravishankar Borgaonkar, Oxford University

COINS Summer School
Mitochi
4 August 2016

Outline

- Cellular Network Architecture
- Security Requirements
- Authentication in 1G to 4G
- Issues related to authentication
- Conclusion

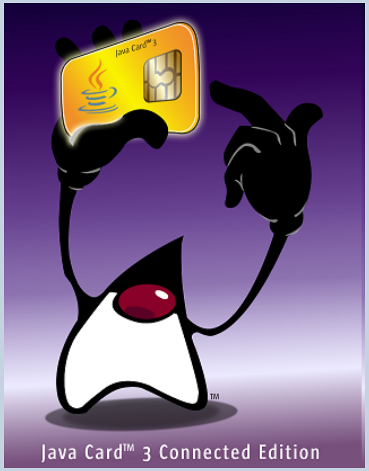
Note: Some resources in this presentation are used from the course I used to teach at TU Berlin with Prof. Jean-Pierre Seifert.

SIM – pillar for authentication

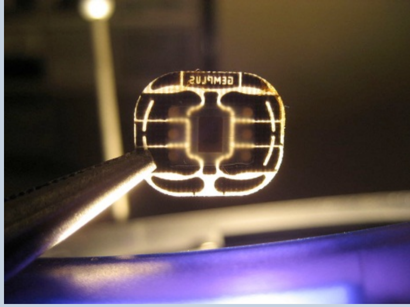
- Subscriber Identity Module
- Universal Integrated Circuit Card (UICC)
    - In GSM, refers as SIM
    - In UMTS system, runs USIM software (entire card is not the USIM)
    - Supports different software modules: ISIM (IMS), CSIM (CDMA)
    - R-UIM (Removable User Identity Module) - CDMA system

Hardware/OS

- Hardware is typically a smartcard punchout (25x15 mm)
  - UICC contains CPU, ROM, RAM, EEPROM, and I/O circuits
- SIM operating systems are either proprietary or Java Card
- Java Card is commonly found on both SIMs and ATM cards
  - Uses a subset of the Java language
  - Optimized byte-code format
  - Applets are "firewalled" from one another



SIM Data (1)

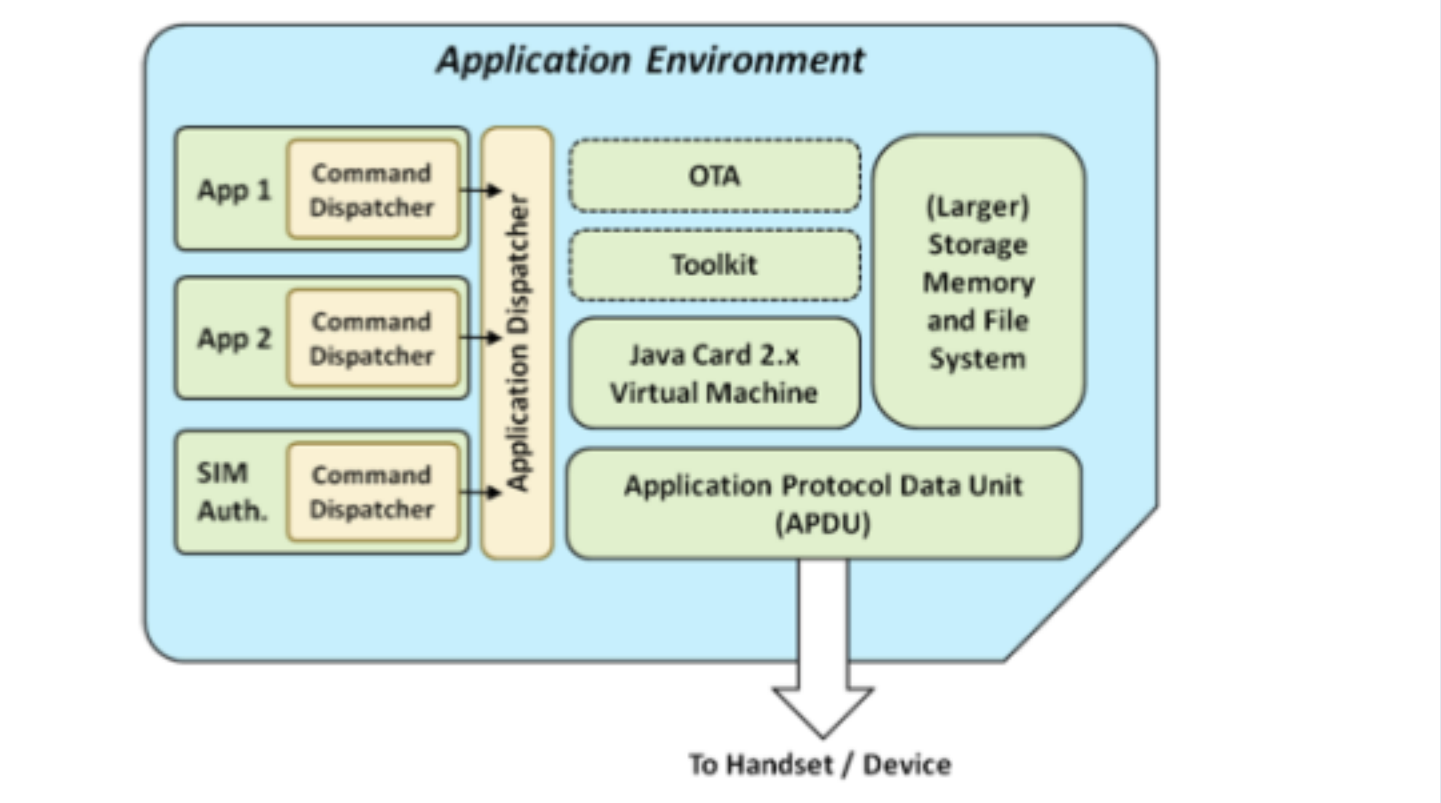


- Integrated Circuit Card ID (ICC-ID) (aka SIM Serial Number - SSN)
  - Uniquely identifies a SIM card (hardware)
  - Conforms to ISO/IEC 7812 (19-20 digits)
- International Mobile Subscriber Identity Module (IMSI)
  - Uniquely identifies the mobile subscriber (15 digits, ITU E.212 standard)
  - MCC (3 digits), MNC (2 or 3 digits), MSIN (9 or 10 digits)
- Authentication Key (K_i)
  - Key shared with provider
  - Never leaves the SIM in any computation
- authentication algorithms performed on-chip

SIM Data (2)

- Location Area Identity (LAI)
  - Stores the last known location area (saves time on power cycle)
- Address book and SMS messages
  - Higher capacity in more advanced cards
  - Have you seen “Inbox full message” in old phones?
- And more ...
  - SMSC number
  - Service Provider Name (SPN)
  - Service Dialing Numbers (SDN)
  - value-added-services

Current SIM architecture



Source: ofcom

DEPARTMENT OF COMPUTER SCIENCE

SIM Application Toolkit

- Before smart phones became popular, the SIM Application Toolkit (STK) was a popular method of deploying applications on mobile phones
    - Allowed for mobile banking applications (and other value added services) to run off the SIM (no handset hardware/OS dependence)
    - Commonly written in Java (for JavaCard) using predefined commands (applications are menu driven)
    - Send data to remote application using SMS
    - OTA update method were eventually incorporated
- STK in UMTS defined as the USIM Application Toolkit (USAT) - 3GPP TS 31.111, security is 3GPP TS 23.048
    - Will new mobile phone OSes make STK and USAT obsolete?

SIM Card Readers

- SIM cards can be connected to a PC for various purposes
- SIM card readers are cheap (~$10-20) or build yourself
  - Provide a serial (TTY) interface (DB9 or USB)
- Allows you to: backup contacts and SMS, see list of previously called numbers, probe keying data to extract K_i ...
- Frequently used for Forensics
  - See NIST “Guidelines on Cell Phone Forensics”, Special Pub 800-101
  - Includes list of SIM tools

Locking SIM and USSD codes

- The SIM card restricts access using two PINs (4-8 digits)
  - PIN 1: If set, the PIN is required to make calls
  - PIN 2: Protects certain network settings
- What happens if you forget your PIN?
  - Commonly, three failed attempts locks the SIM
- What are the ways to unlock SIM? USSD attack story?
- Unlocking a locked SIM card
  - Personal Unblocking Code (PUC) or Personal Unblocking Key (PUK)
  - Commonly acquired from the network provider
  - Ten failed attempts often permanently locks the SIM

Security in SIM cards

- Identity and Access control (IMSI, PIN code)
- Authentication to network operator (Ki, A3)
- Confidentiality (Kc, A8)
- Anonymity (TMSI)
- SIM application toolkit

SIM Cloning

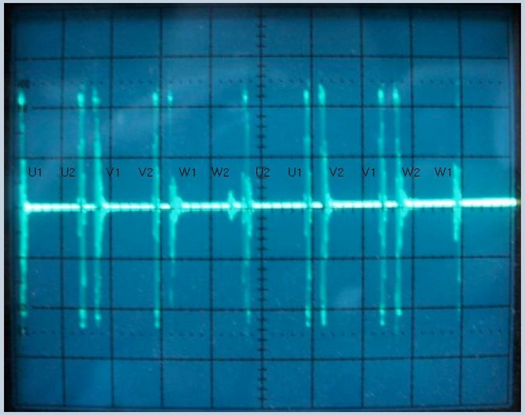
- SIM Cloning is the process of extracting Ki from one SIM card and writing it onto another.
  - It less frequently than before due to updates in crypto algorithms and authentication protocols, but is still possible in some cases.
  - Many software and hardware cloners exist

- Why clone? - steal service, forensics, SIM/network lock circumvention, *not* eavesdropping (but knowing K_i helps)

- Network can detect cloned SIMs; protections vary
  - Simultaneous calls cannot occur
  - Can network detect the cloned SIM card?
  - Who gets the SMS in case of cloning?

Power Analysis

- SIM cards are smart cards, therefore, they are also vulnerable to power analysis attacks (requires special equipment).
  - Hardware implementations cause power consumption of the chip to become a side-channel to determine the key used to perform some cryptographic algorithms.
  - See work by Kocher et al. (Differential Power Analysis)
- Goal is to recover Ki from the analysis



Security attacks

SIM Cloning (1998)

- Comp128 algorithm leaked
- Reverse engineered & cryptanalyzed

SIM toolkit attacks

- Fuzzing SMS
- Send premium SMS

Cracking SIM Update keys

- Recover DES OTA keys
- Singed malicious applets with key

Changing Telco world

- Goal achieved in lat 25 years - “ billions users connecting every continent”
- Next goal- “Connecting billions of devices (m2m devices, vehicles, IoT devices)”
- SIM to USIM to eSIM
- Embedded SIM vs Soft SIM
- New security architecture

Embedded SIM

Designed for M2M devices

Non-removable

No Soft/virtual SIM

New security standard

No change in authentication / encryption to the operator

Security architecture for remote provisioning

2G, 3G and 4G Architecture

Network Components (GSM)

- HLR stores records of all mobile subscribers
- MSC/VLR connect wired and wireless components of the network and responsible handoffs
- BS communicate with mobile devices over radio link
- MS is a subscriber's mobile device

HLR

- Stores records of mobile subscribers and their current location serving area

- Authentication Center (AuC)
  - International Mobile Subscriber Identity (IMSI) of all subscribers
  - Stores crypto keys (K_i) and performs operations for authentication

- Device level authentication
  - Equipment Identity Register (EIR)

- Includes a blacklist (e.g., for stolen phones)
  - International Mobile Equipment Identity (IMEI) identifies a mobile device

MSC and VLR

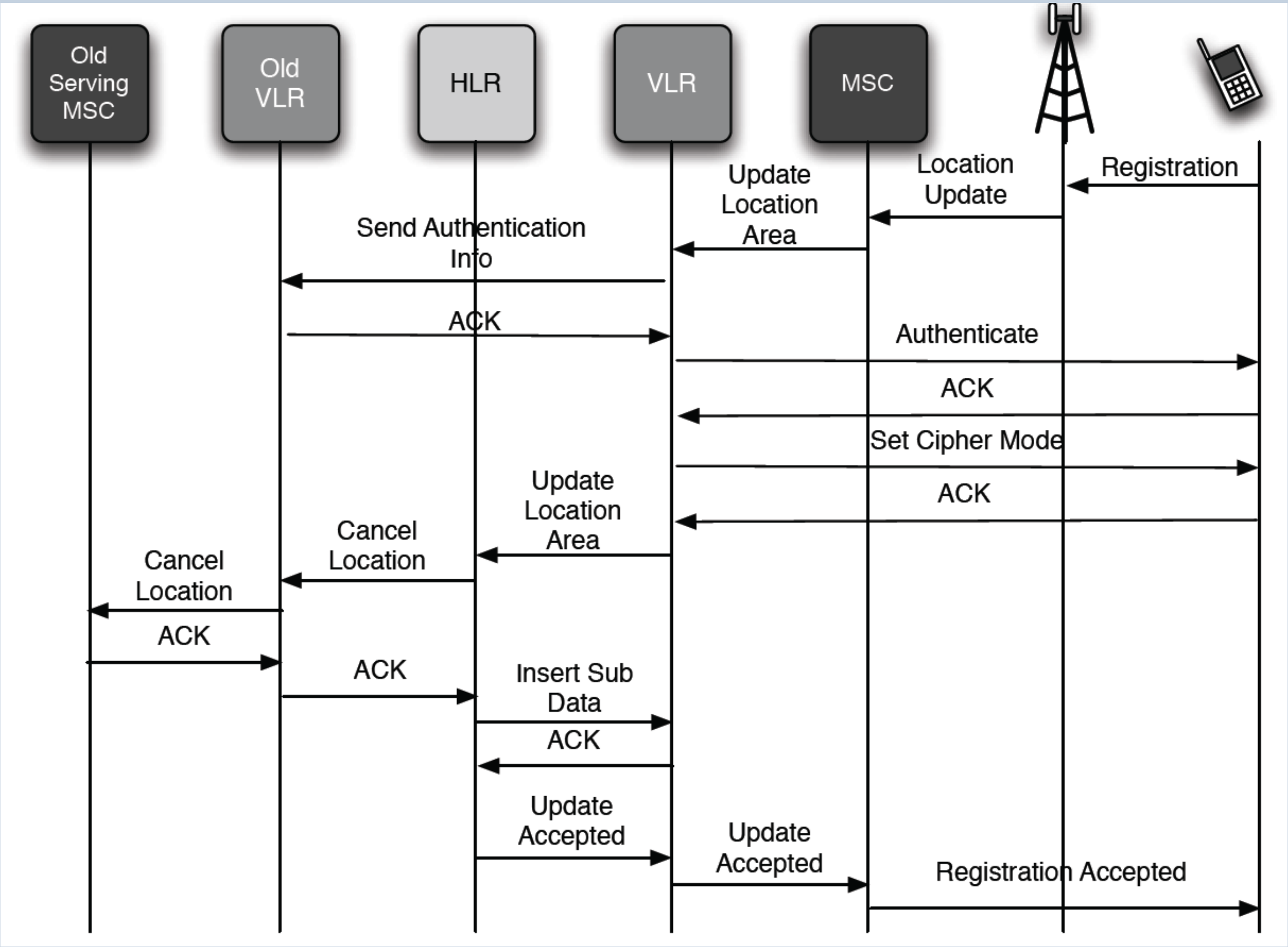
- The Mobile Switching Center (MSC) delivers circuit switched telephony traffic within the cellular network
    - Gateway MSC is the term given to an MSC bridging the cellular network and another network, e.g., Public Switched Telephone Network (PSTN) or another cellular network.
    - Serving MSC is the term given to an MSC currently serving an MS
    - The MSC also assists handoffs between base stations and billing
- The Visitor Location Register (VLR) caches information from the HLR for fast lookup by an MSC
    - A particular VLR may serve multiple MSC components (not always)
    - The VLR stores “triplets” from HLR (for authentication)

BSS

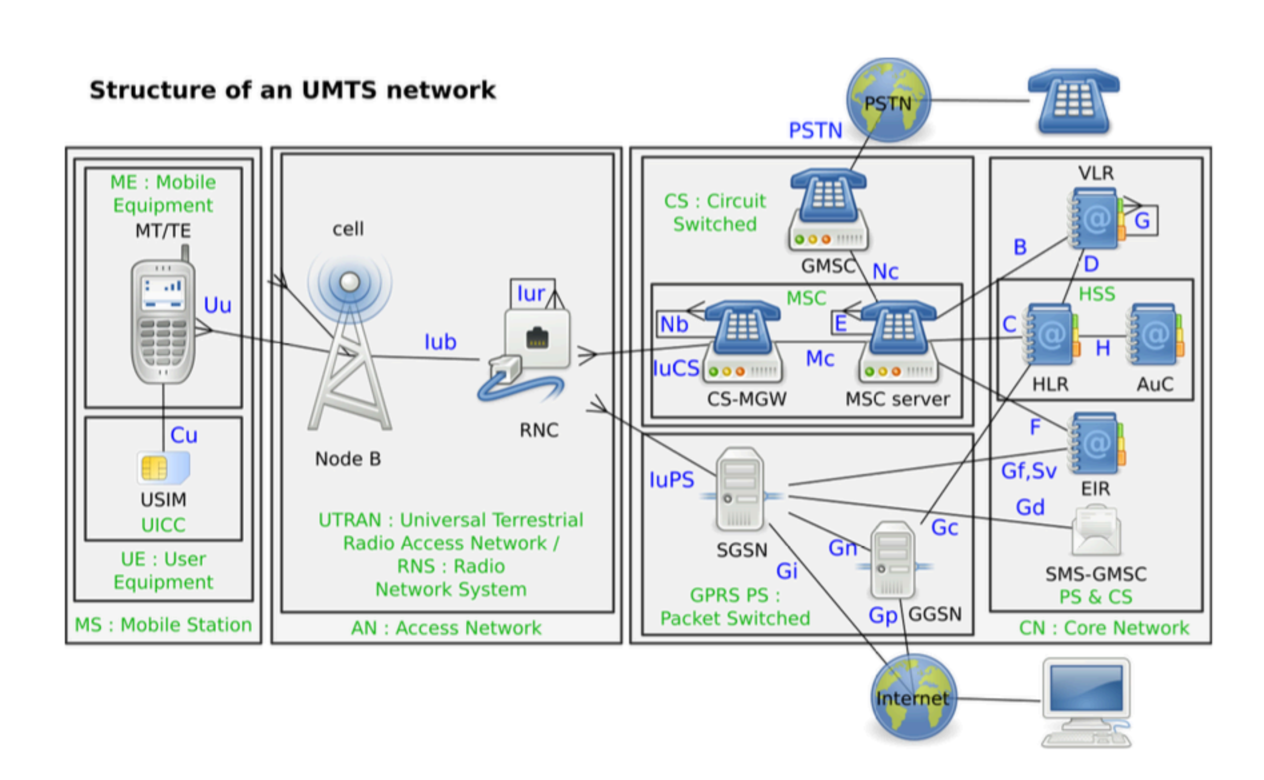
- Base Station Subsystem (BSS) links mobile devices to the core network and consists of
  - Base Transceiver Station (BTS): the transmission radio (multiple directional antennas dividing the cell into sectors)
  - Base Station Controller (BSC): intelligence for radios (include scheduling and encryption), controlling one or more BTSs

- Generally referred as base station and often grouped into *Location Areas* (LAs) corresponding to geographic regions
  - Devices can move between base stations in an LA without re-registering (handover)

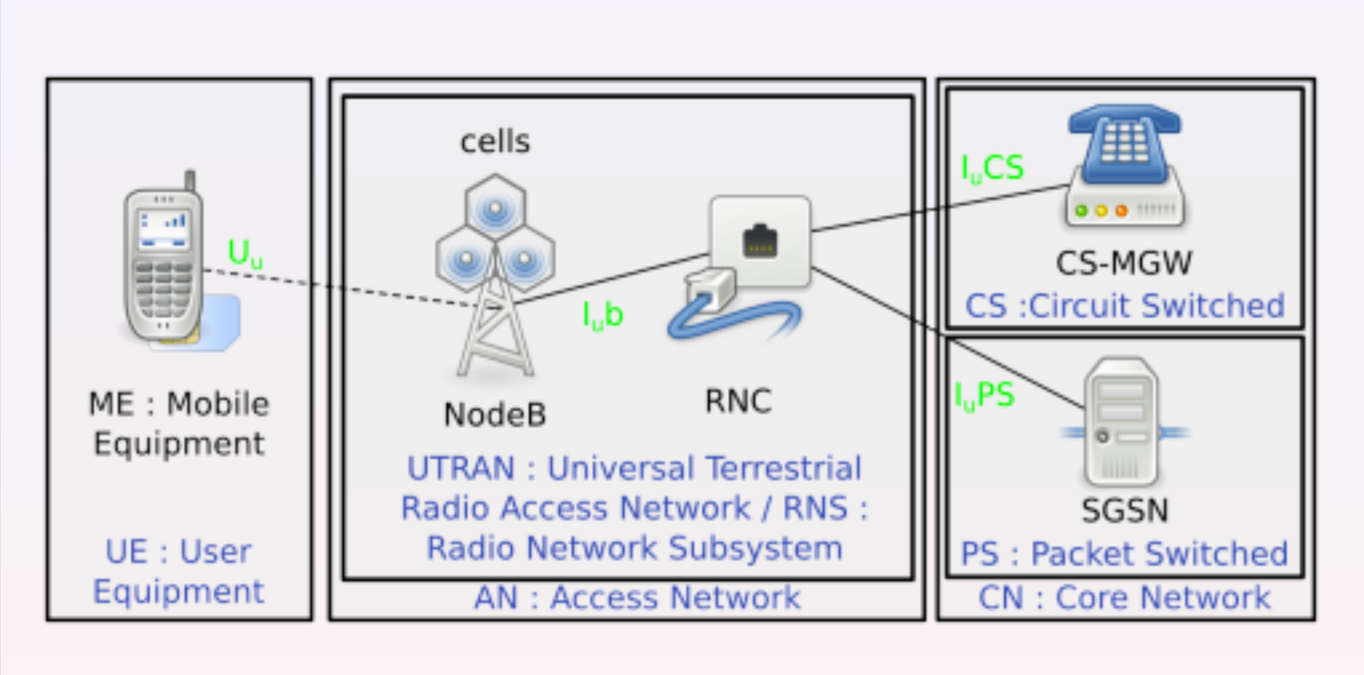
Phone Registration



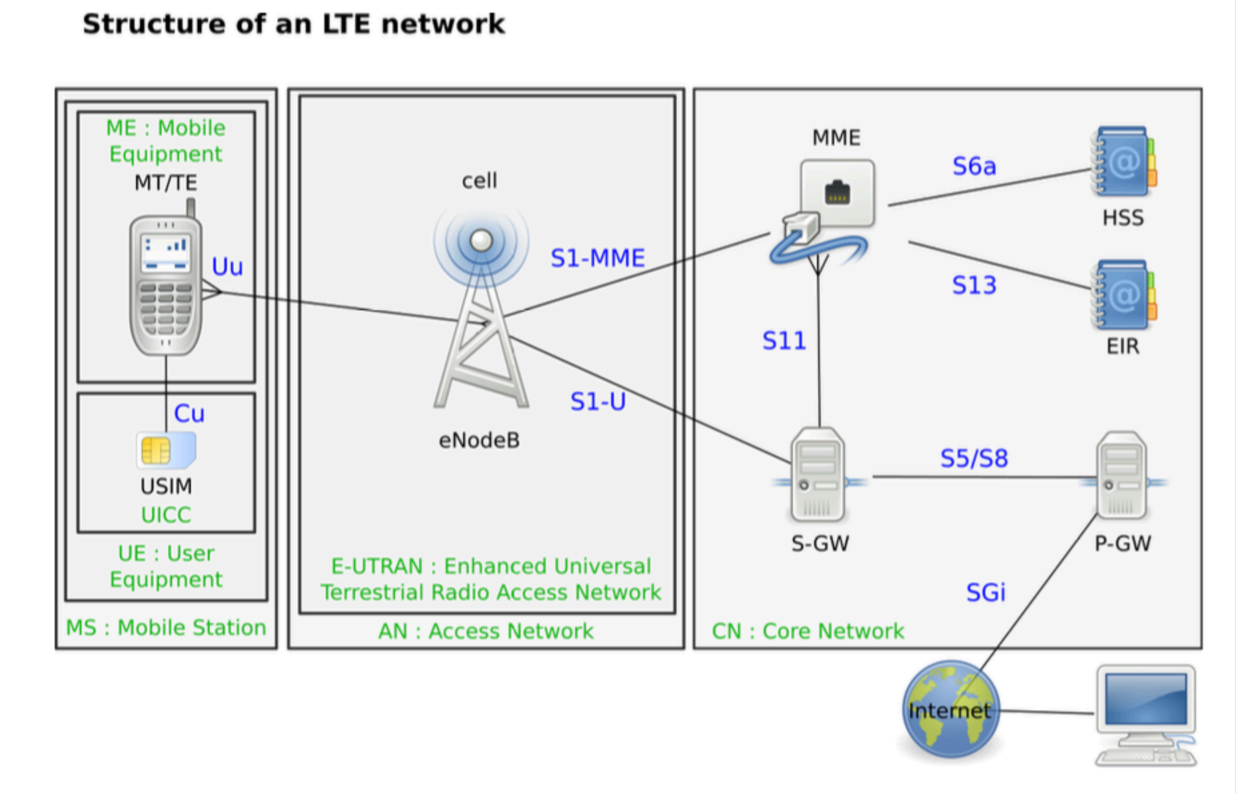
3G Architecture and Components



3G Architecture and Components (Simplified)



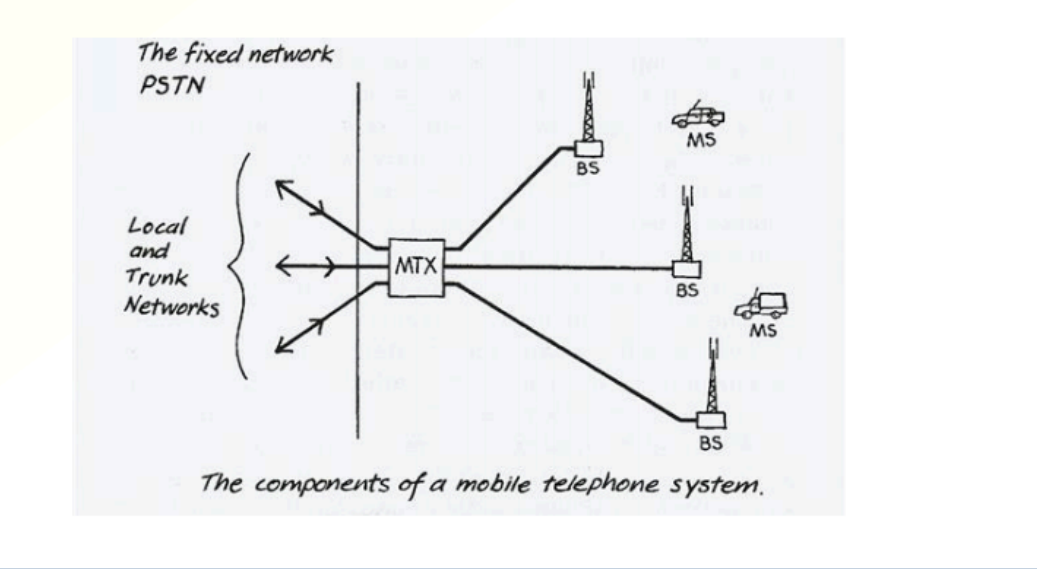
4G Architecture



Authentication in 1G, GSM, 3G

Authentication in 1G networks

- No authentication
- No encryption
- What are possible threats?

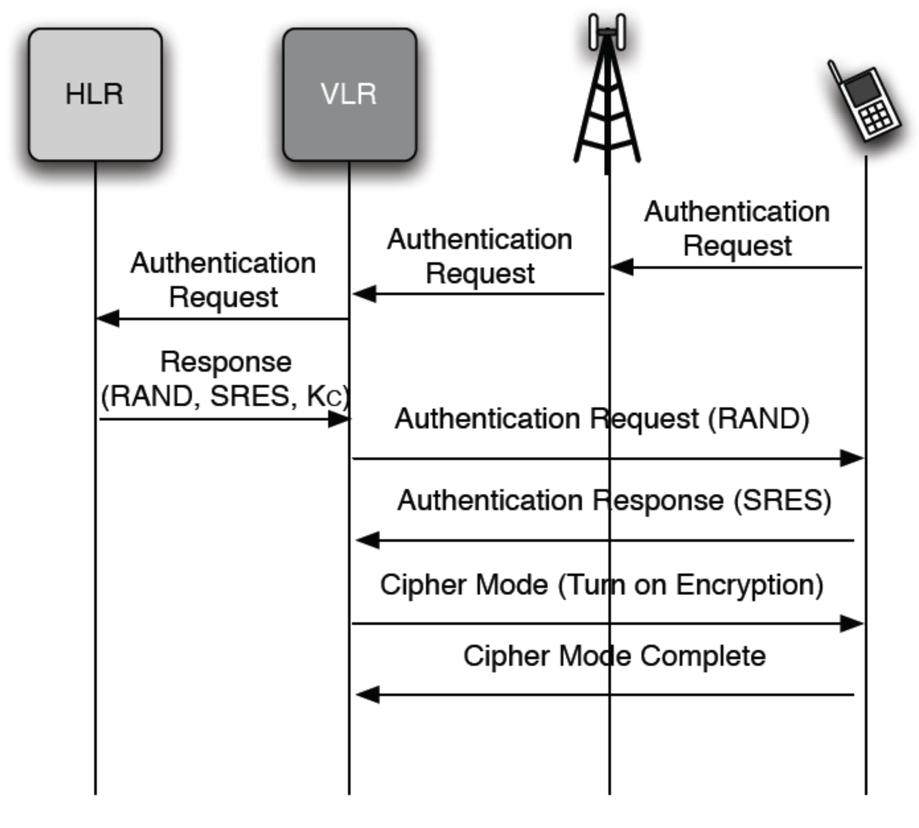


The components of a mobile telephone system.

Source : Ericsson

Phone Authentication (GSM)

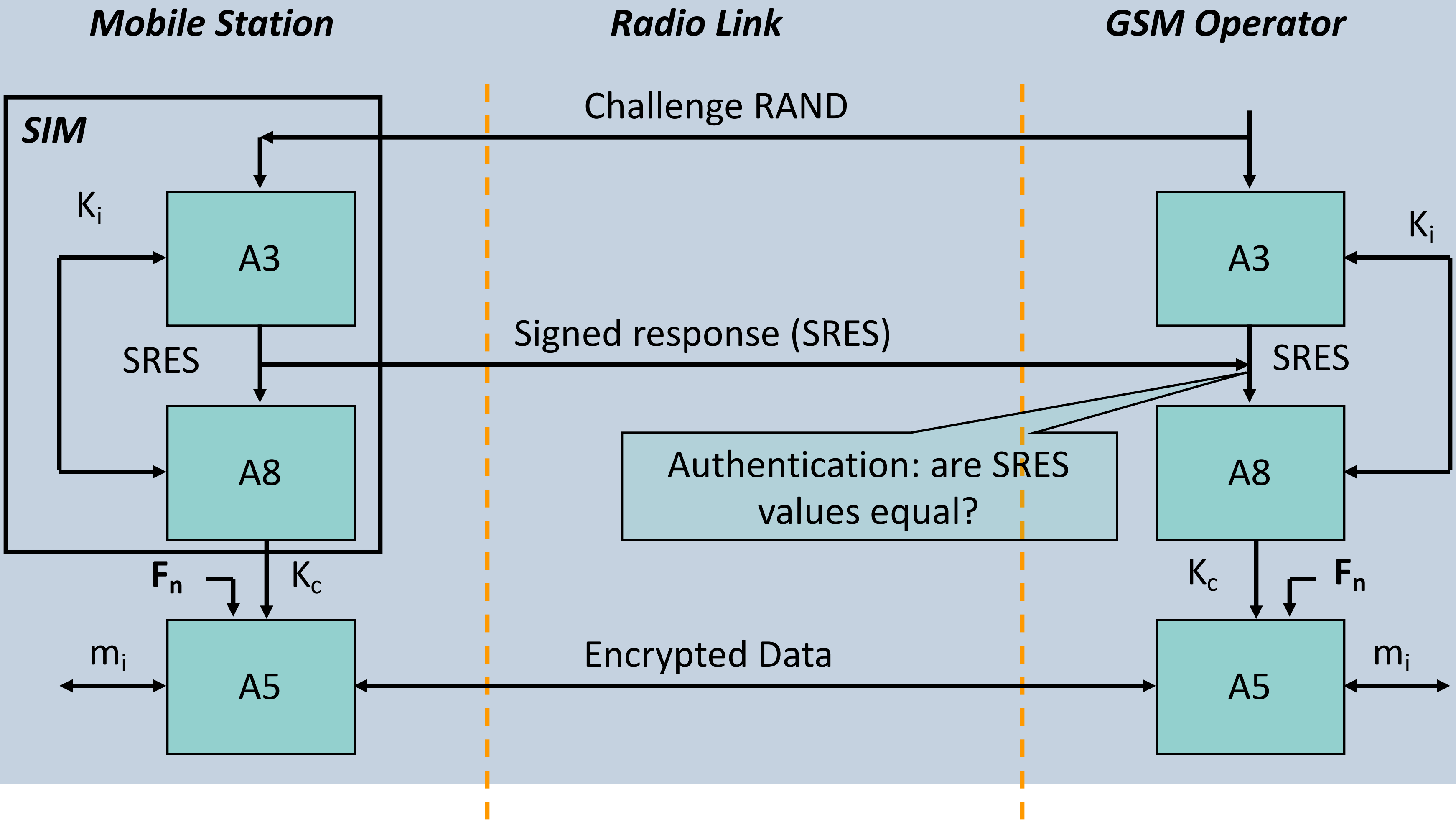
- three algorithms (based on 128-bit key, K_i)
  - A3 - Authentication
  - A8 - Generates cipher key
  - A5 - Ciphering data
- VLR retrieves triplets from HLR (AuC)
  - RAND - random challenge
  - SRES - expected response
  - [SRES = A3(K_i, RAND), 32 bits]
  - K_c - corresponding cipher key
  - [K_c = A8(K_i, RAND), 64 bits]
- Only the HLR and SIM card know K_i


HLR
VLR
Authentication Request
Authentication Request
Authentication Request
Response (RAND, SRES, Kc)
Authentication Request (RAND)
Authentication Response (SRES)
Cipher Mode (Turn on Encryption)
Cipher Mode Complete

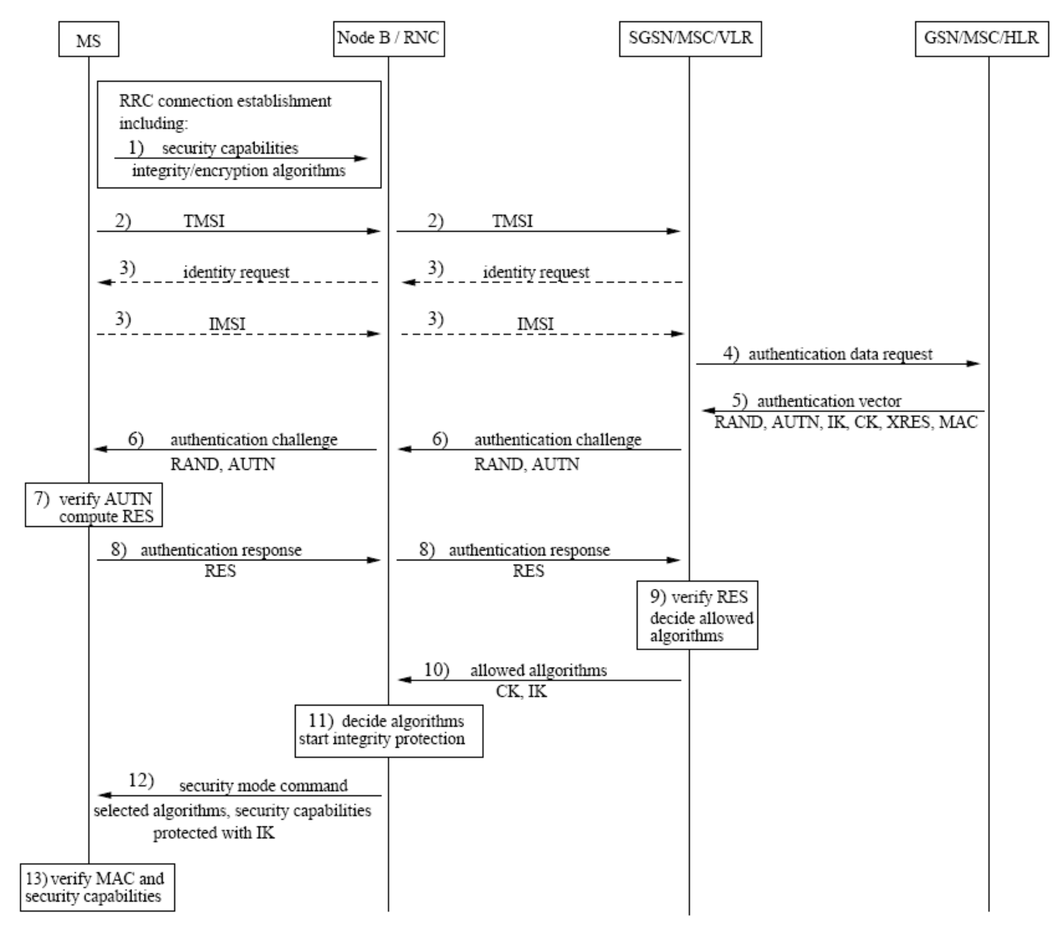
Security issues in GSM

- IMSI is transferred in plaintext
- IMEI can be requested in plaintext and not authenticated
- No mutual authentication
- Encryption ends at the base station

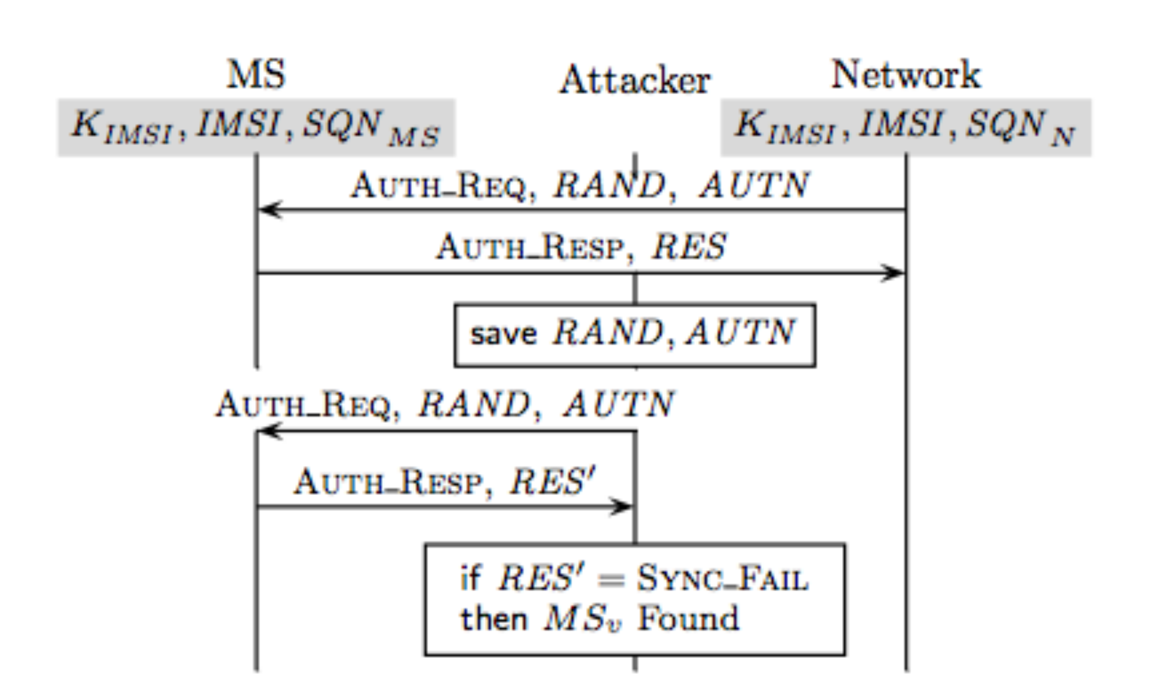
Authentication/Encryption in GSM



Authentication and Key Agreement in UMTS


MS
Node B / RNC
SGSN/MSC/VLR
GSN/MSC/HLR
RRC connection establishment including:
1) security capabilities
integrity/encryption algorithms
2) TMSI
2) TMSI
3) identity request
3) identity request
3) IMSI
3) IMSI
4) authentication data request
5) authentication vector
RAND, AUTN, IK, CK, XRES, MAC
6) authentication challenge
RAND, AUTN
6) authentication challenge
RAND, AUTN
7) verify AUTN
compute RES
8) authentication response
RES
8) authentication response
RES
9) verify RES
decide allowed algorithms
10) allowed allgorithms
CK, IK
11) decide algorithms
start integrity protection
12) security mode command
selected algorithms, security capabilities
protected with IK
13) verify MAC and
security capabilities

AKA protocol issue



Source: Arapinis M, Mancini L, Ritter E, Ryan M, Golde N, Redon K and Borgaonkar R (2012), *"New Privacy Issues in Mobile Telephony: Fix and Verification"*, In Proceedings of the 2012 ACM conference on Computer and communications security. , pp. 205-216

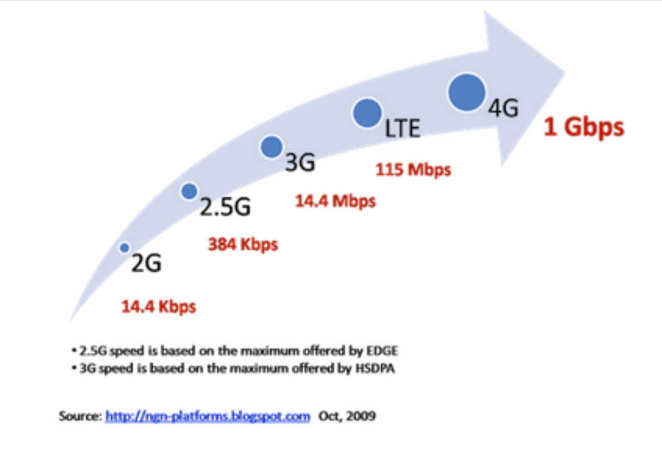
Security issues in UMTS

- IMSI is transferred in plaintext
- IMEI can be requested in plaintext and not authenticated
- Encryption ends at RNC but still not end to end
- Privacy issue – allows tracking of subscribers

Authentication in 4G

Need of LTE Networks

- Higher data rates
  - upto 100 Mbps
- High level of security
  - stronger than GSM/3G
- Enhanced quality of service
- Capabilities for internetworking with non 3GPP systems (for example WiMAX)



- 2.5G speed is based on the maximum offered by EDGE
- 3G speed is based on the maximum offered by HSDPA

Source: http://ngn-platforms.blogspot.com Oct, 2009

LTE/SAE Networks

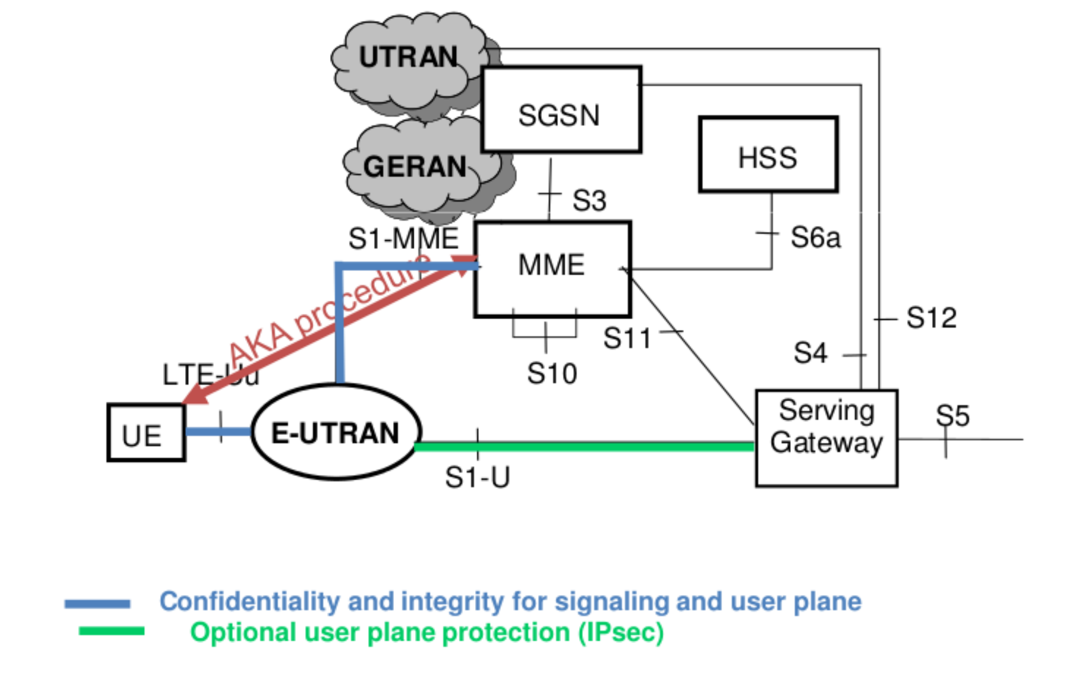
- Radio network E-UTRAN with a new radio interface
- Flat IP based core network EPC

- E-UTRAN : Evolved Universal Terrestrial Radio Access Network)
- EPC : Evolved Packet Core
- LTE : Long Term Evolution
- SAE: System Architecture Evolution

LTE Security Features

- Reuse of 3G AKA
- Reuse of 3G USIM (2G SIM is not allowed)
- Extended key hierarchy
  - To keep security breaches local
- More complex internetworking security
- Additional security for eNodeB (compared to NB in 3G and BTS in GSM)

LTE Network Architecture

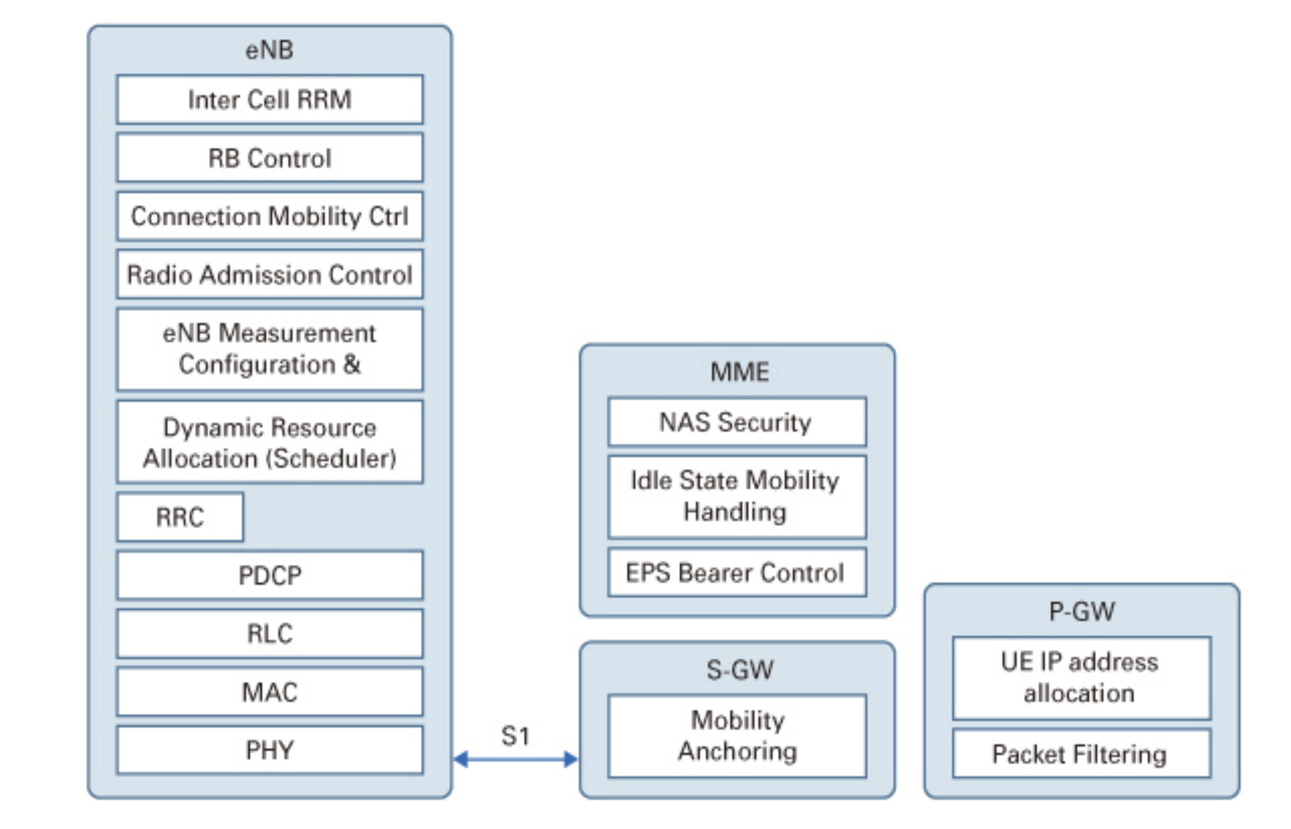

UTRAN
SGSN
GERAN
HSS
S3
S1-MME
S6a
MME
AKA procedure
S12
S11
LTE-Uu
S10
S4
UE
E-UTRAN
Serving Gateway
S5
S1-U
Confidentiality and integrity for signaling and user plane
Optional user plane protection (IPsec)

Source: ETSI presentation, Charles Brookson – Chairman ETSI OCG Security

New Network Components

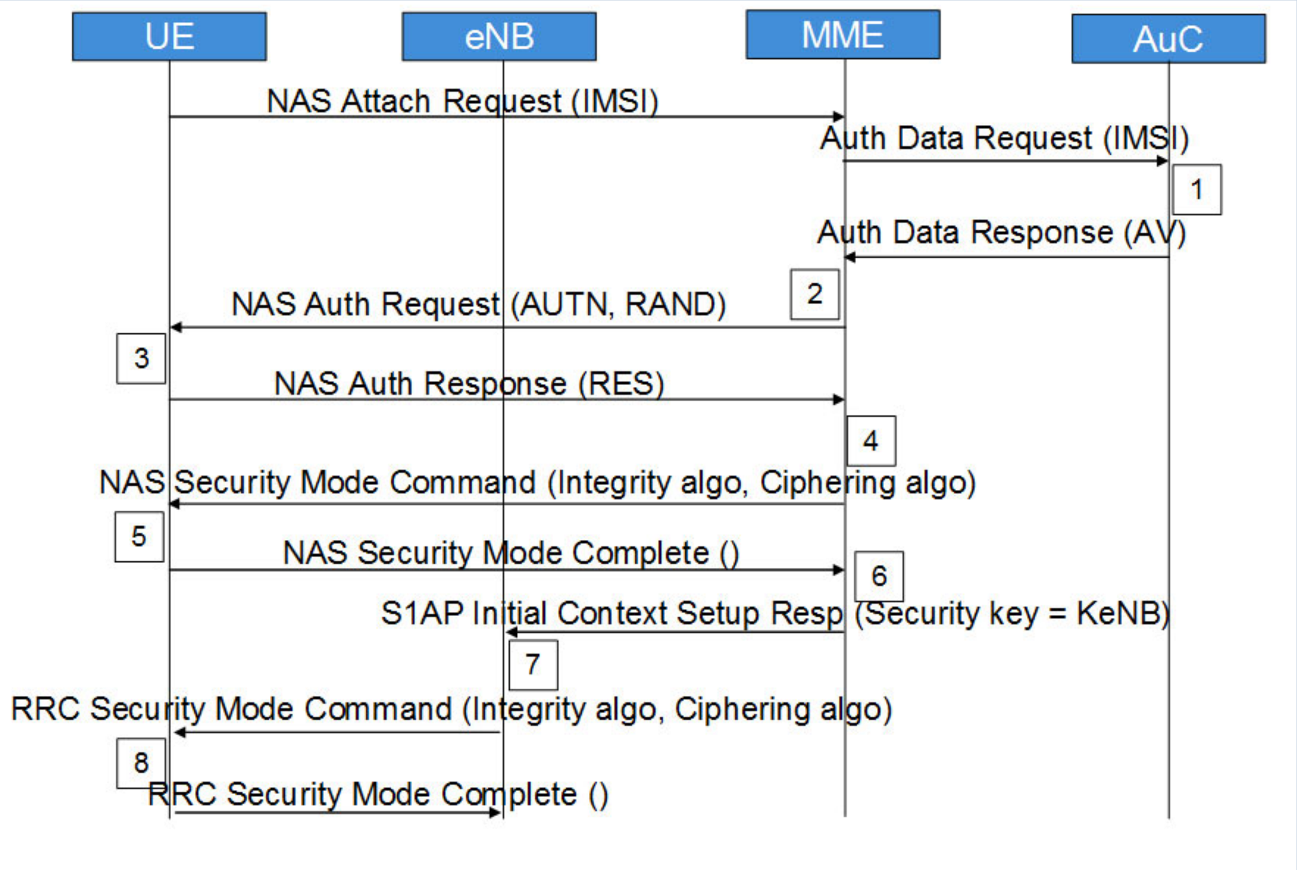
- MME – Mobile Management Entity
  - Key control node
  - User authentication, autherization, NAS signalling, lawful interception etc.
- eNB
  - Radio resource management
  - IP header compression and encryption
- Serving Gateway
  - Routes and forwards user data packets
  - Acts as anchor for mobillity between LTE and other systems.

Roles of components

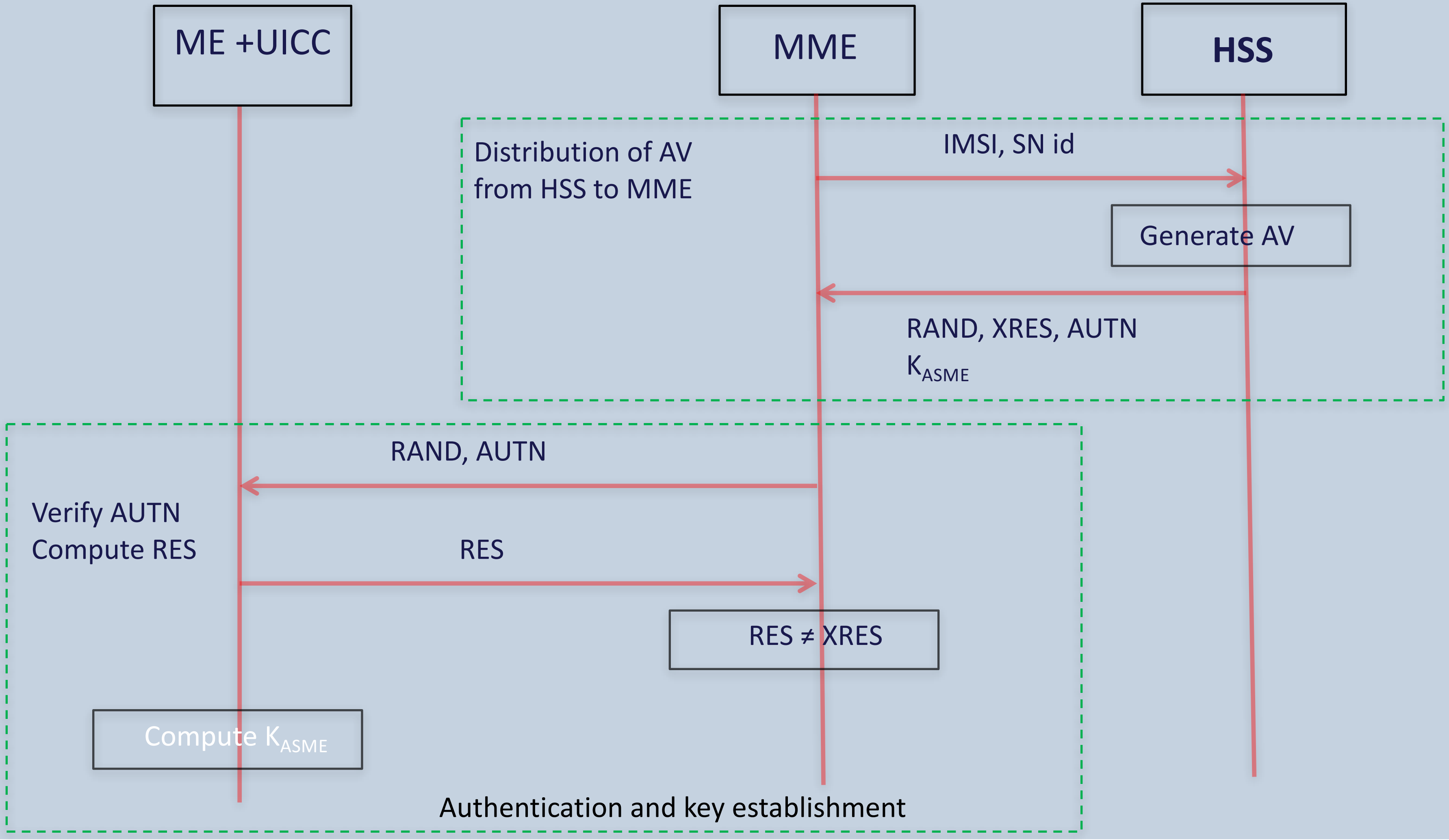


Source: Artiza Networks

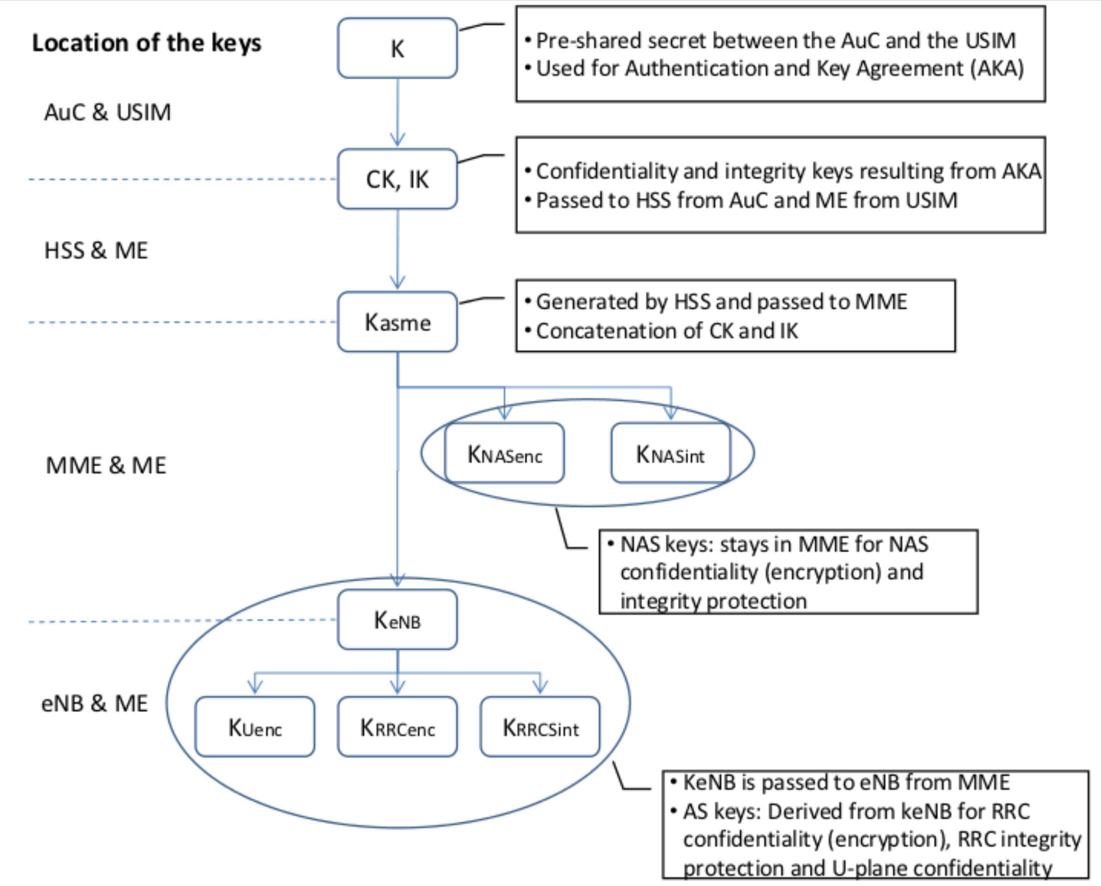
Authentication and Key Agreement


UE
eNB
MME
AuC
NAS Attach Request (IMSI)
Auth Data Request (IMSI)
1
Auth Data Response (AV)
2
NAS Auth Request (AUTN, RAND)
3
NAS Auth Response (RES)
4
NAS Security Mode Command (Integrity algo, Ciphering algo)
5
NAS Security Mode Complete ()
6
S1AP Initial Context Setup Resp (Security key = KeNB)
7
RRC Security Mode Command (Integrity algo, Ciphering algo)
8
RRC Security Mode Complete ()

LTE AKA protocol (simplified)



Key Hierarchy



- Pre-shared secret between the AuC and the USIM
- Used for Authentication and Key Agreement (AKA)

- Confidentiality and integrity keys resulting from AKA
- Passed to HSS from AuC and ME from USIM

- Generated by HSS and passed to MME
- Concatenation of CK and IK

- NAS keys: stays in MME for NAS confidentiality (encryption) and integrity protection

- KeNB is passed to eNB from MME
- AS keys: Derived from keNB for RRC confidentiality (encryption), RRC integrity protection and U-plane confidentiality

Motivation for Key Hierarchy

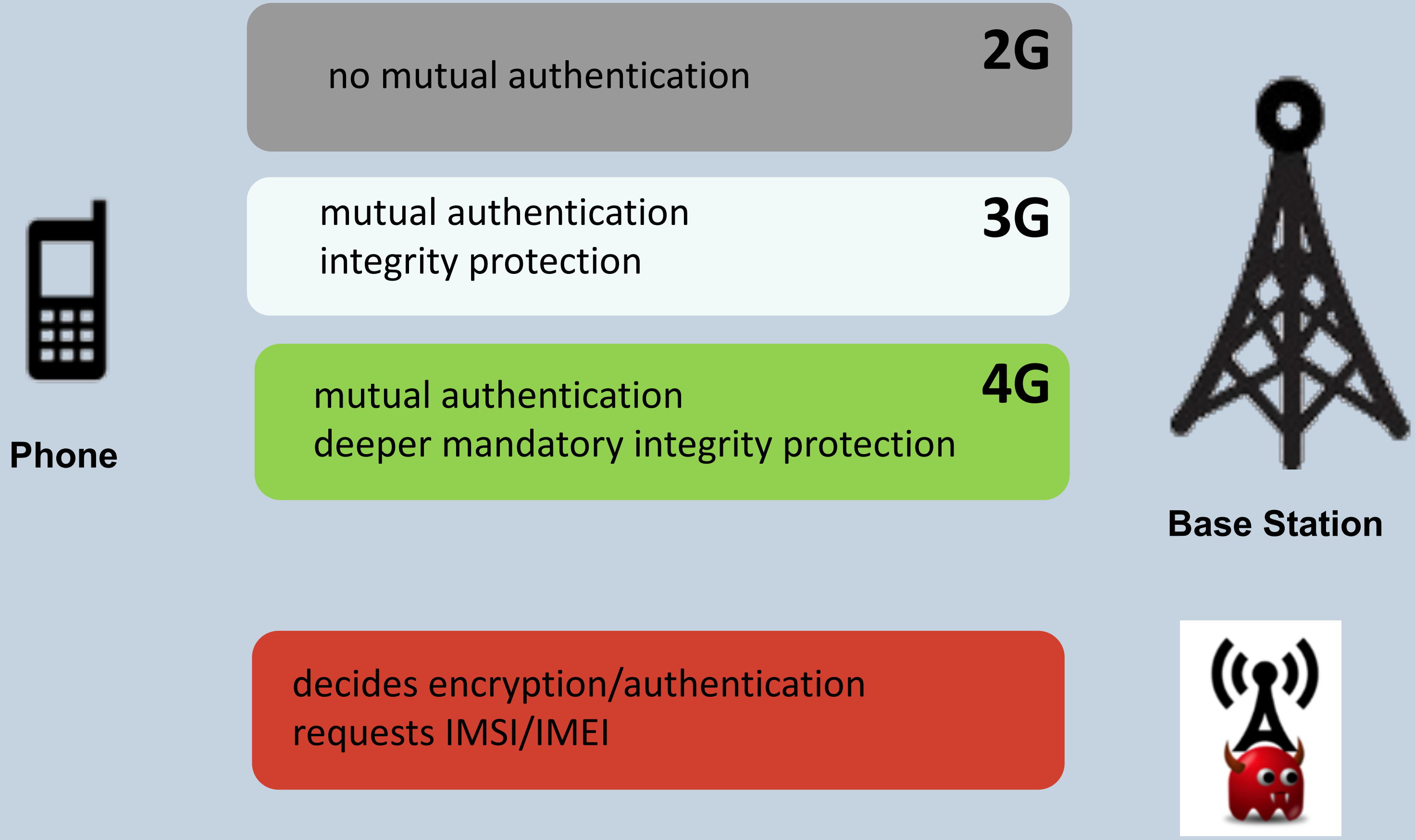
- Cryptographic key separation
  - Keys from one context can not be used in other
- Key renewal
  - Minimize distribution of same secret key elements
  - Key freshness is important for secured systems

Security Algorithms

- Two sets of algorithms – what If one breaks up, other one as backup
- AES and Snow 3G algorithms are choosen
- Both are kept possibly different, cracking of one algorithms should not reveal other one
- Integrity Algorithms
  - 128-EIA1 Snow 3G
  - 128-EIA2 AES
- Ciphering Algorithms
  - 128-EEA1 Snow 3G
  - 128-EEA2 AES
- Key size 128 bit but possibility of extending to 256 bits
- Third set based on Chinese ZUC algorithm is developed

Attacks in 2G, 3G, and 4G

Security evolution in mobile networks



Phone

2G
no mutual authentication

3G
mutual authentication
integrity protection

4G
mutual authentication
deeper mandatory integrity protection

Base Station

decides encryption/authentication
requests IMSI/IMEI

Security aspects

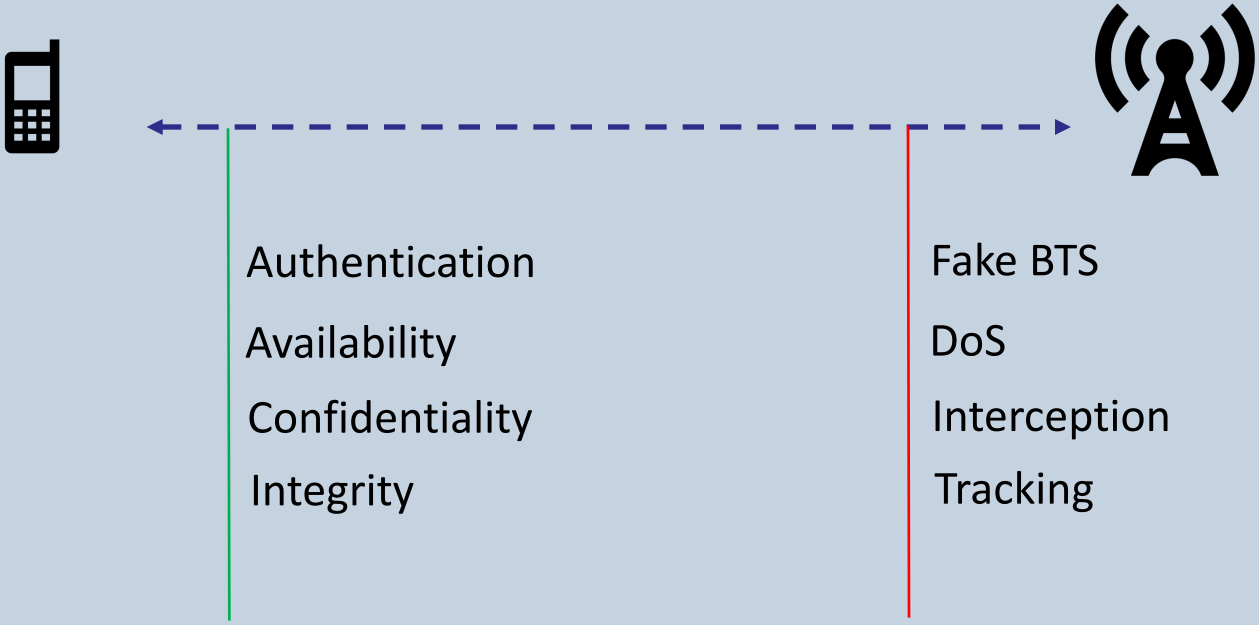
Authentication

Availability

Confidentiality

Integrity

Security aspects and attacks



Authentication

Availability

Confidentiality

Integrity

Fake BTS

DoS

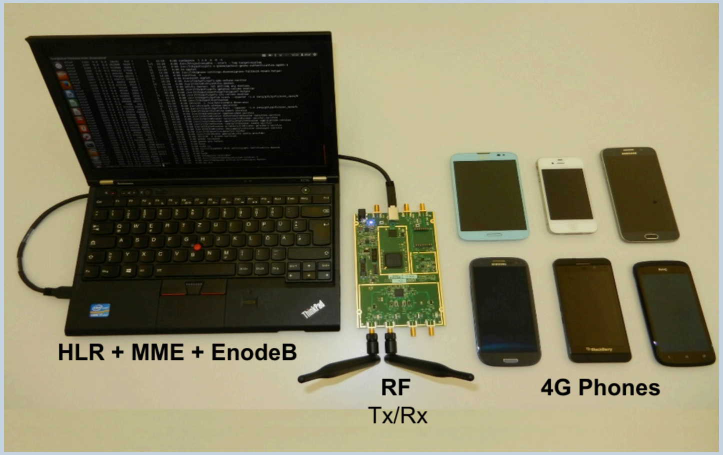
Interception

Tracking

Security tradeoffs play essential role in protocol design.

Low cost attacking infrastructure

- 2G/3G/4G* network setup cost < 1000 USD
  - Open source software & hardware
  - USRP, Osmocom, OpenBTS, OpenLTE, etc



- IMSI catcher device problem

- Targeted attacks from illegal actors

- Almost no detection capabilities for the end-users

Emerging attack examples

IMSI catchers (1)

- Exploit weakness in authentication methods
- Location tracking and interception
- Protection for ‘active attacks’ not considered
- Lack of security indicator implementation

Small cellular base-sta
homeland security app

3G-GSM TACTICAL INTERCEPTION & TARGET LOCATION

Implementation issues on RAN

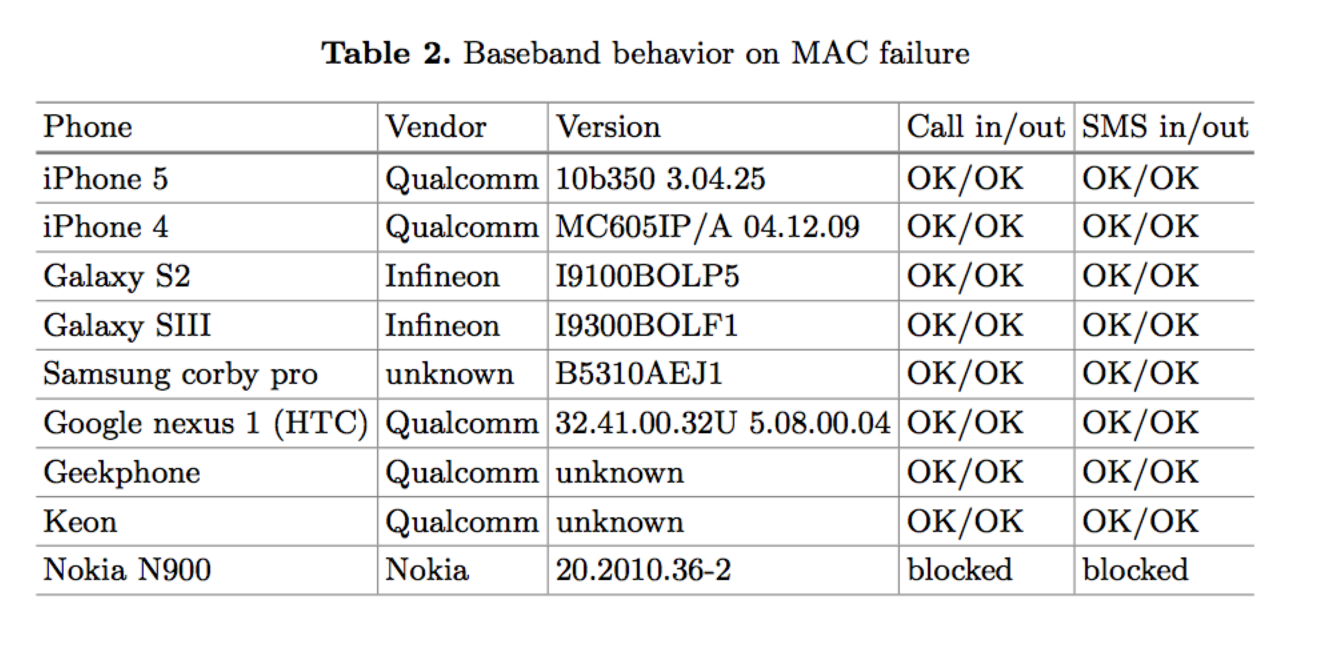


Table 2. Baseband behavior on MAC failure

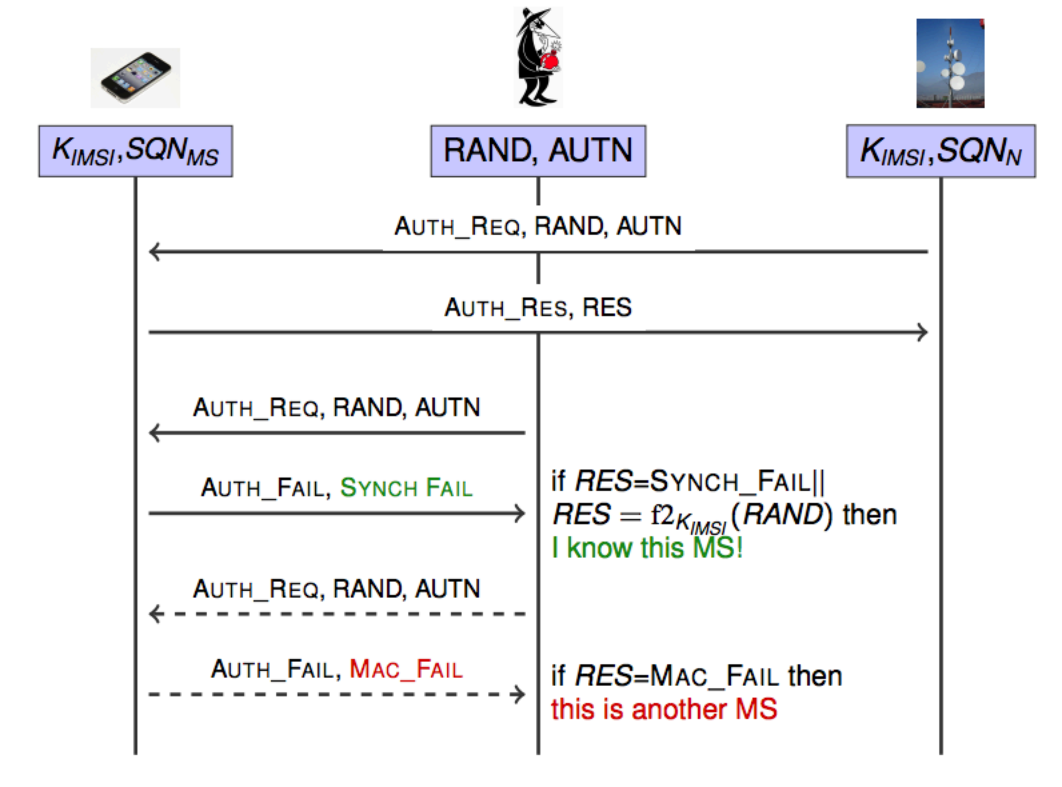
Phone	Vendor	Version	Call in/out	SMS in/out
iPhone 5	Qualcomm	10b350 3.04.25	OK/OK	OK/OK
iPhone 4	Qualcomm	MC605IP/A 04.12.09	OK/OK	OK/OK
Galaxy S2	Infineon	I9100BOLP5	OK/OK	OK/OK
Galaxy SIII	Infineon	I9300BOLF1	OK/OK	OK/OK
Samsung corby pro	unknown	B5310AEJ1	OK/OK	OK/OK
Google nexus 1 (HTC)	Qualcomm	32.41.00.32U 5.08.00.04	OK/OK	OK/OK
Geekphone	Qualcomm	unknown	OK/OK	OK/OK
Keon	Qualcomm	unknown	OK/OK	OK/OK
Nokia N900	Nokia	20.2010.36-2	blocked	blocked

From TS 124.008 v11.8.0 : If MAC failure, then phone should not communication with BTS (2G)

Table from the paper "Implementing an Affordable and Effective GSM IMSI Catcher with 3G Authentication"

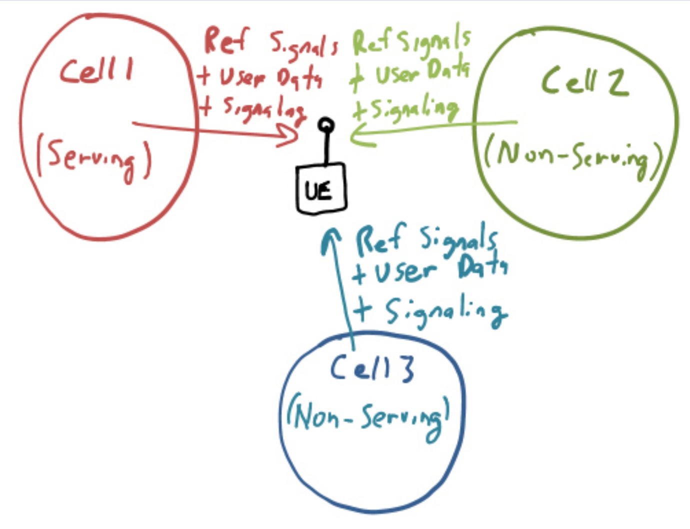
3G AKA vulnerability(2)

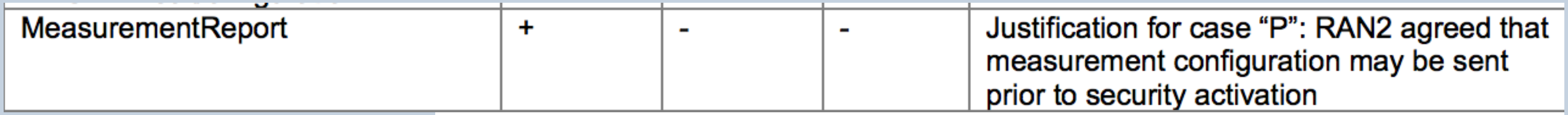
- Linkability attack by Arpanis et al
- Affects in 4G as well



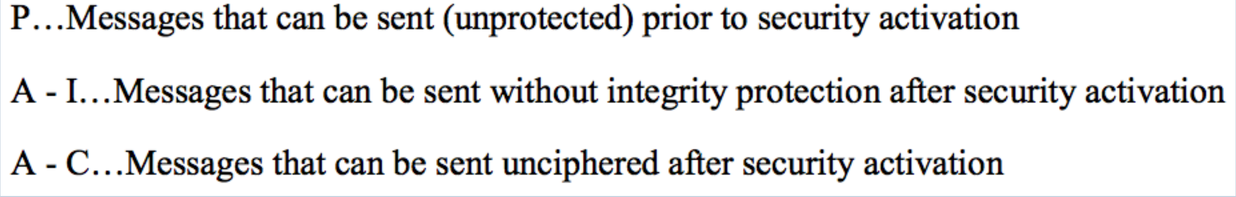
3GPP Specification issues

- RRC protocol – 3GPP TS 36.331
- ‘UE Measurement Report’ messages
- Necessary for handovers & troubleshooting
- No authentication for messages
- Reports not encrypted





MeasurementReport	+	-	-	Justification for case “P”: RAN2 agreed that measurement configuration may be sent prior to security activation

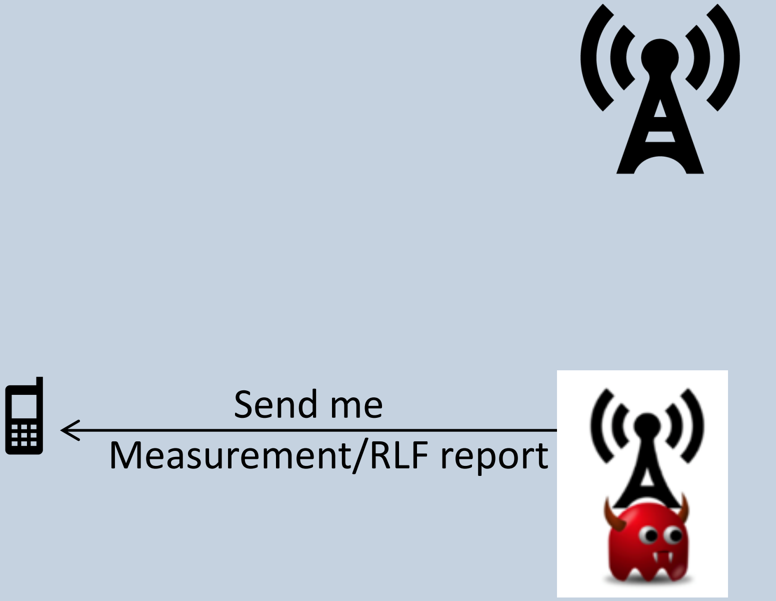


P…Messages that can be sent (unprotected) prior to security activation

A - I…Messages that can be sent without integrity protection after security activation

A - C…Messages that can be sent unciphered after security activation

Vulnerabilities in the feature



Send me Measurement/RLF report

active attacker

Specification

UE measurement reports

- Requests not authenticated
- Reports are not encrypted

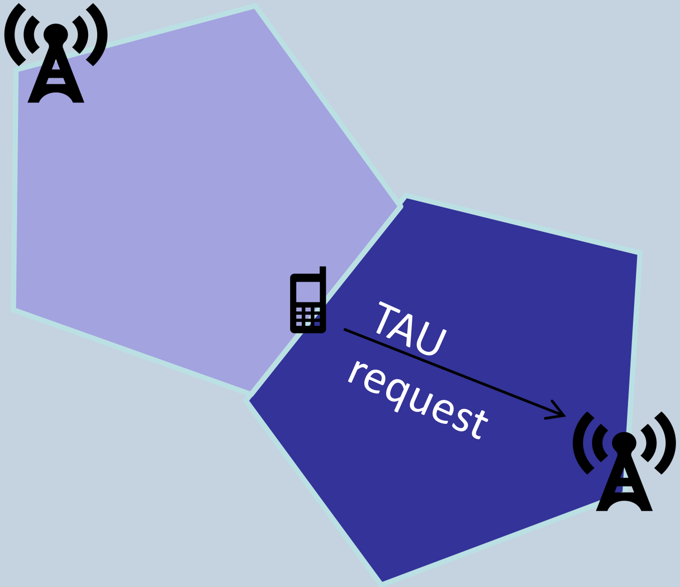
Implementations

RLF reports

- Requests not authenticated
- Reports are not encrypted
- All baseband vendors

4G Feature: Mobility Management

EMM protocol – 3GPP TS 36.331



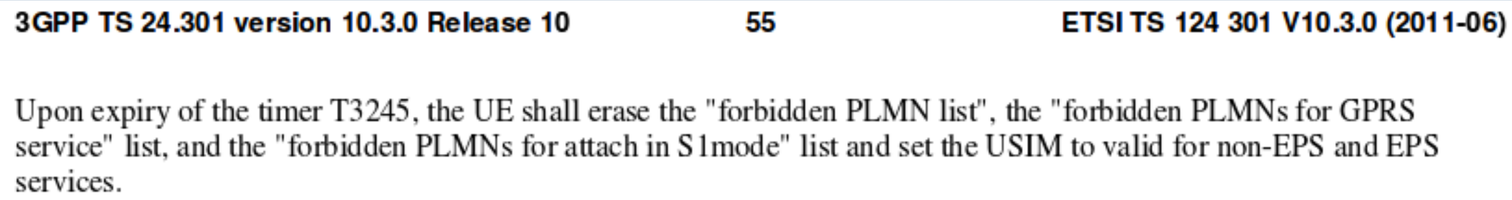
Tracking Area Update (TAU) procedure

- During TAU, MME & UE agree on network mode (2G/3G/4G)
- "TAU Reject" used to reject some services services (e.g., 4G) to UE

Specification vulnerability: Reject messages are not integrity protected

3GPP Specification issues

- EMM protocol – 3GPP TS 36.331
- ‘Tracking Area Update Reject’ messages
- Necessary for UE mobility
- No integrity protection for reject messages
- Recovery mechanism not effective

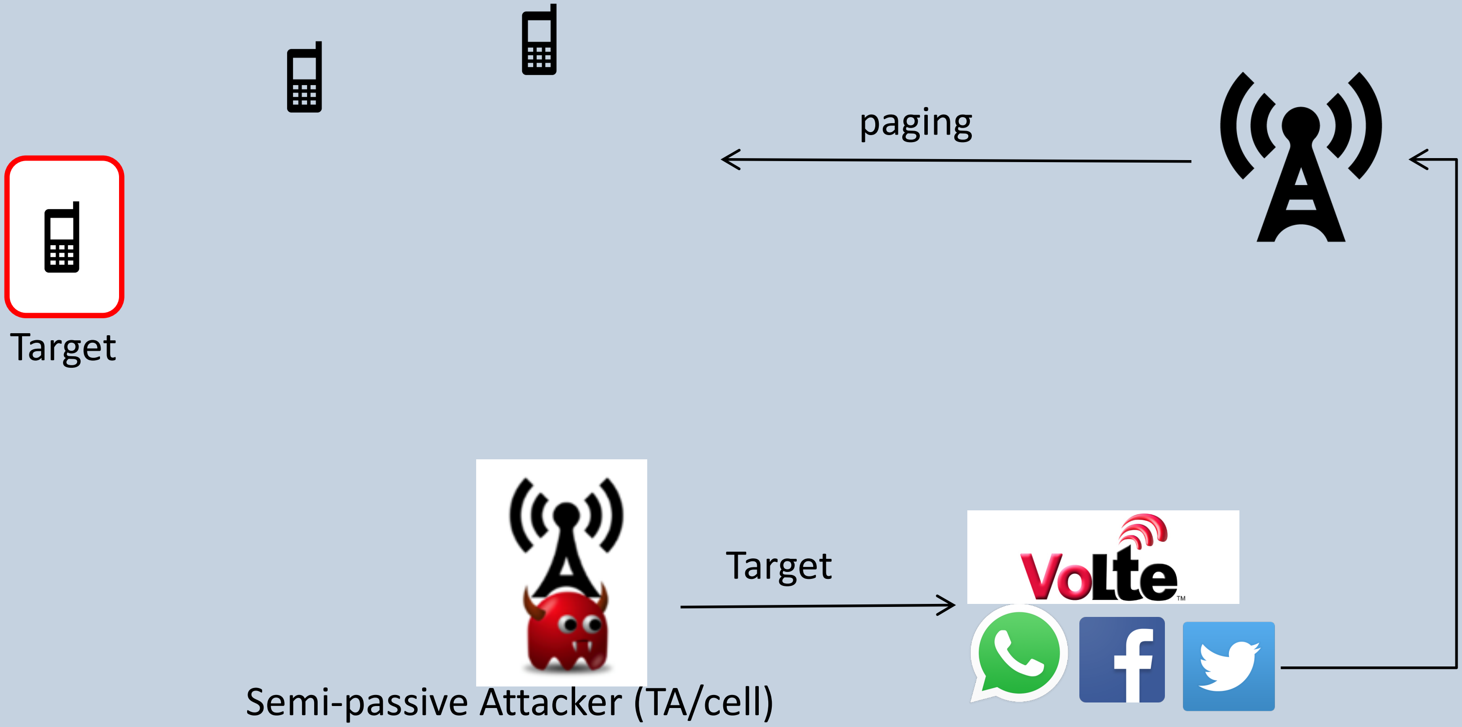


3GPP TS 24.301 version 10.3.0 Release 10 **55** **ETSI TS 124 301 V10.3.0 (2011-06)**

Upon expiry of the timer T3245, the UE shall erase the "forbidden PLMN list", the "forbidden PLMNs for GPRS service" list, and the "forbidden PLMNs for attach in S1mode" list and set the USIM to valid for non-EPS and EPS services.

Practical Attacks with low cost tools

Location Leaks: tracking subscriber coarse level



paging

Target

Target

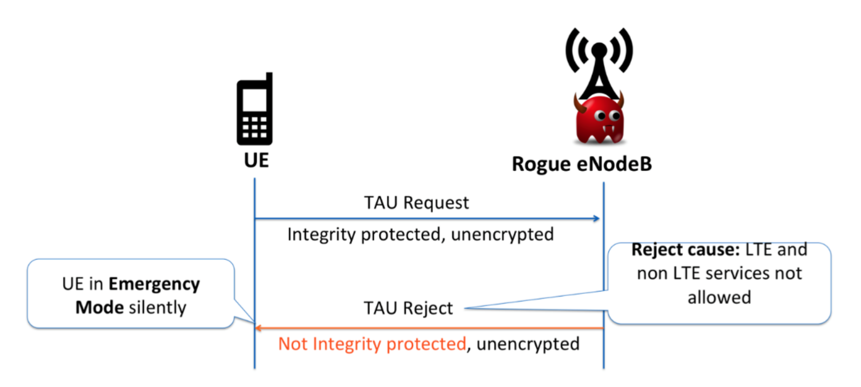
Semi-passive Attacker (TA/cell)

Mapping GUTI to Social Identity

Location Accuracy: 2 Sq. Km

DoS Attacks

- Downgrade to non-LTE network services (2G/3G)
- Deny all services (2G/3G/4G)
- Deny selected services (block incoming calls)
- GSM – IMSI detach , RACH flood
- Flooding DOS attacks towards HLR
- Jamming attacks

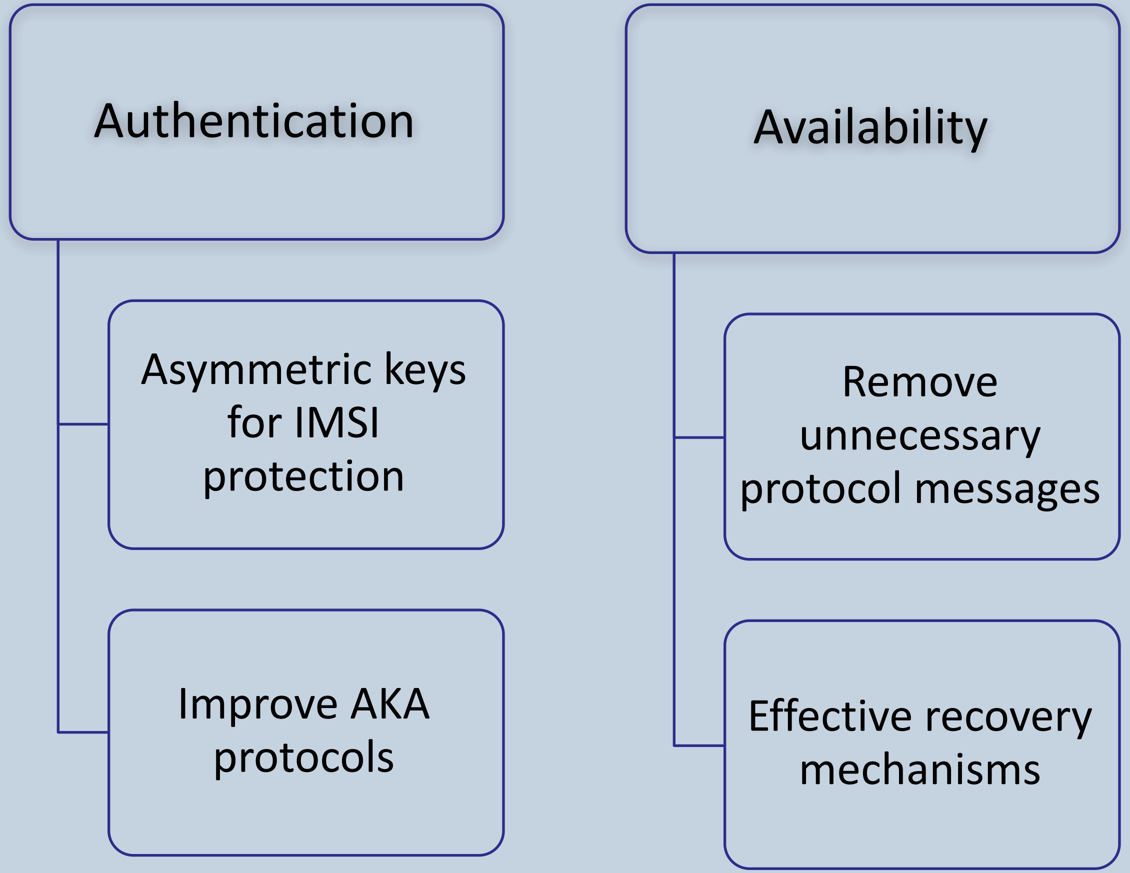

UE
Rogue eNodeB
TAU Request
Integrity protected, unencrypted
Reject cause: LTE and non LTE services not allowed
UE in Emergency Mode silently
TAU Reject
Not Integrity protected, unencrypted

Reasons for different vulnerabilities

Trade of between security and

- Performance
- Availability
- Functionality
- Attacking cost

5G Networks Perspective



Authentication

Asymmetric keys for IMSI protection

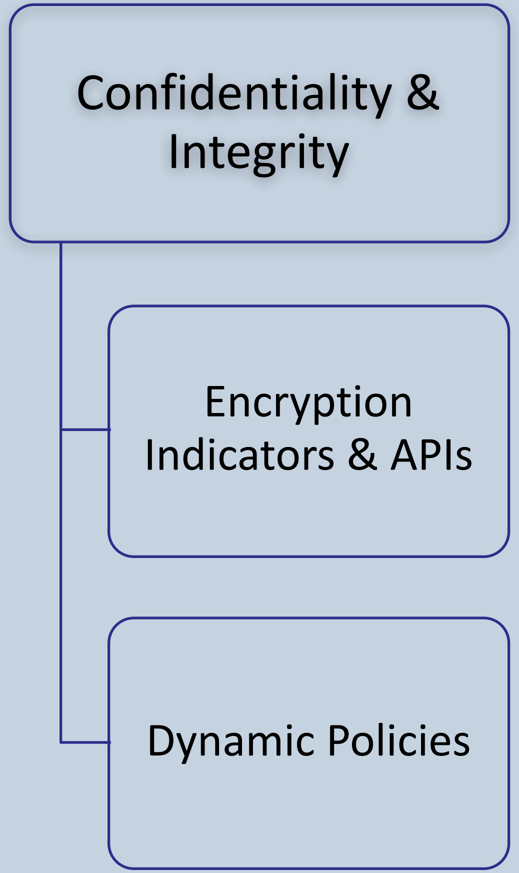
Improve AKA protocols

Availability

Remove unnecessary protocol messages

Effective recovery mechanisms

5G Networks Perspective


Confidentiality & Integrity
Encryption Indicators & APIs
Dynamic Policies