RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: TECH-RO3

LTE Security – How Good Is It?

Jeffrey Cichonski

IT Specialist (Security)
National Institute of Standards & Technology
@jchonski

Joshua Franklin

IT Specialist (Security)
National Institute of Standards & Technology
@thejoshpit

#RSAC

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Objectives

- Discussion of LTE standards
- Description of LTE technology
- Exploration of LTE's protection mechanisms
- Enumeration of threats to LTE
- How good is LTE security?

Context of Research

- The Public Safety Communications Research (PSCR) program is joint effort between NTIA & NIST
  - Located in Boulder, CO
- PSCR investigates methods to make public safety communications systems interoperable, secure, and to ensure it meets the needs of US public safety personnel
  - Researching the applicability of LTE in public safety communications

What is LTE

- LTE – Long Term Evolution
  - Evolutionary step from GSM to UMTS
- 4th generation cellular technology standard from the 3rd Generation Partnership Project (3GPP)
- Deployed worldwide and installations are rapidly increasing
- LTE is completely packet-switched
- Technology to provide increased data rates

3GPP Standards & Evolution

3GPP

atis

CCSA

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

ARIB
Association of Radio Industries and Businesses

ETSI

- 2G GSM
- 2.5G EDGE
- 3G UMTS
- 3.5G HSPA
- 4G LTE

Note: Simplified for brevity

RSA Conference 2015

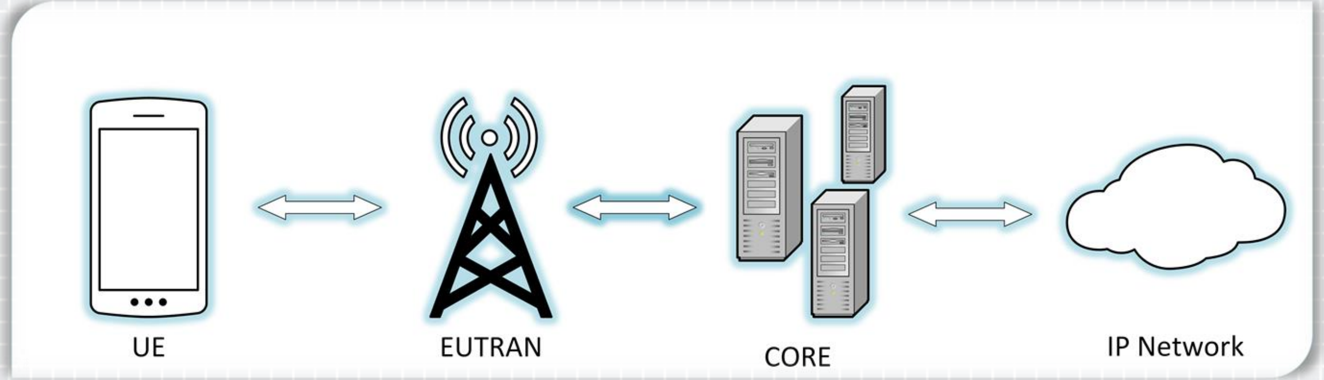
San Francisco | April 20-24 | Moscone Center

#RSAC

LTE Technology Overview

The Basics

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

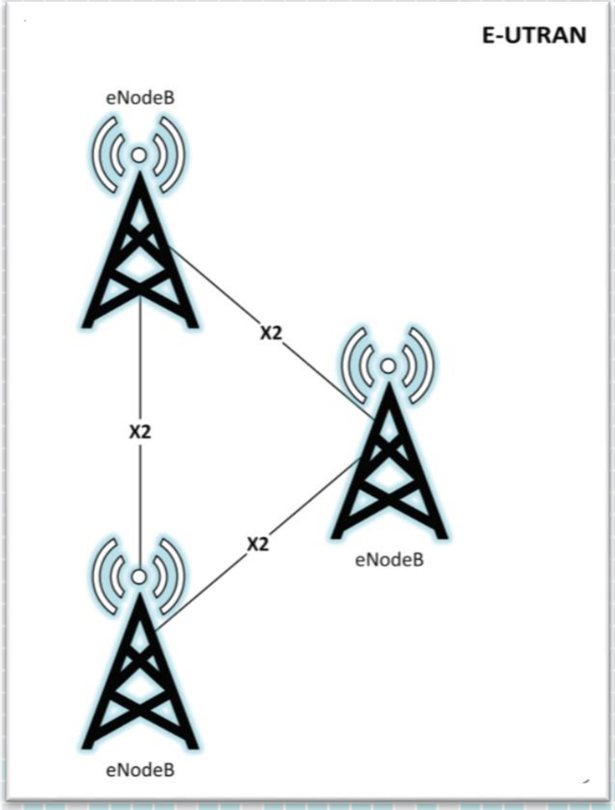


Mobile Device

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

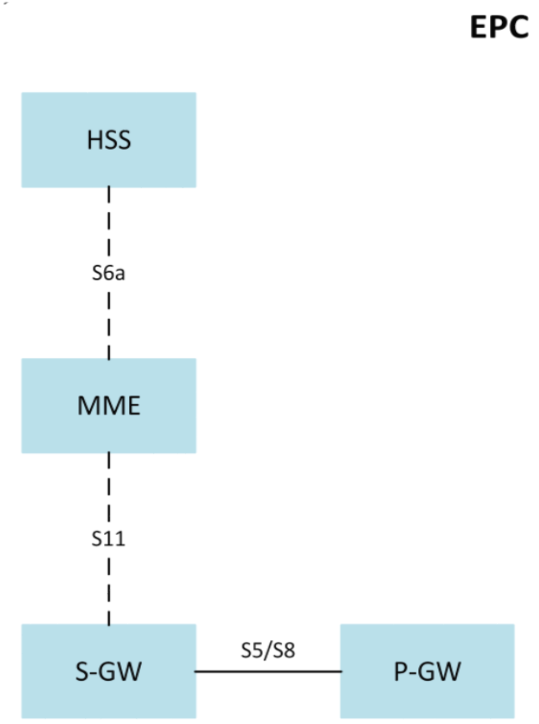
The Evolved Universal Terrestrial Radio Access Network (E-UTRAN)

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



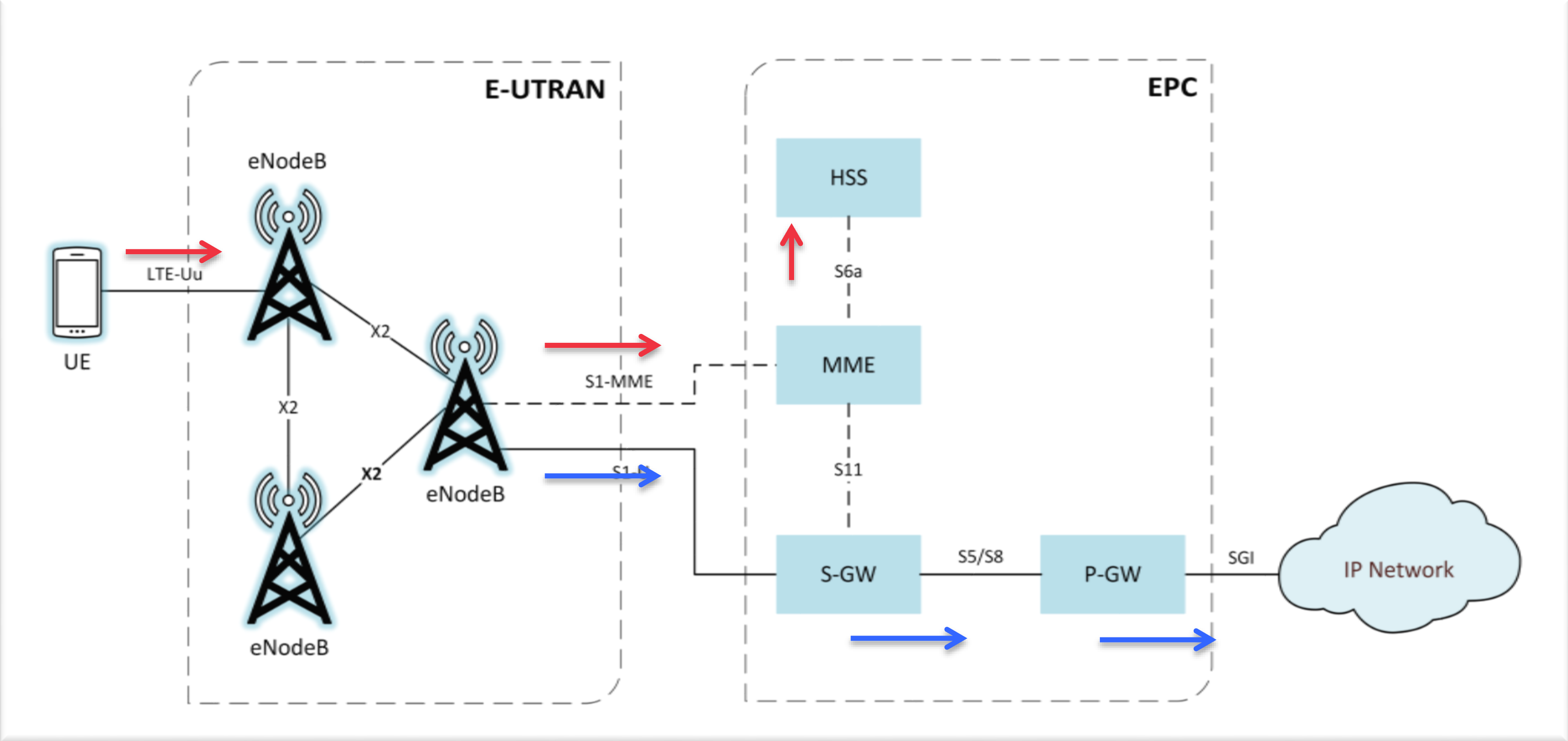
Evolved Packet Core (EPC)

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



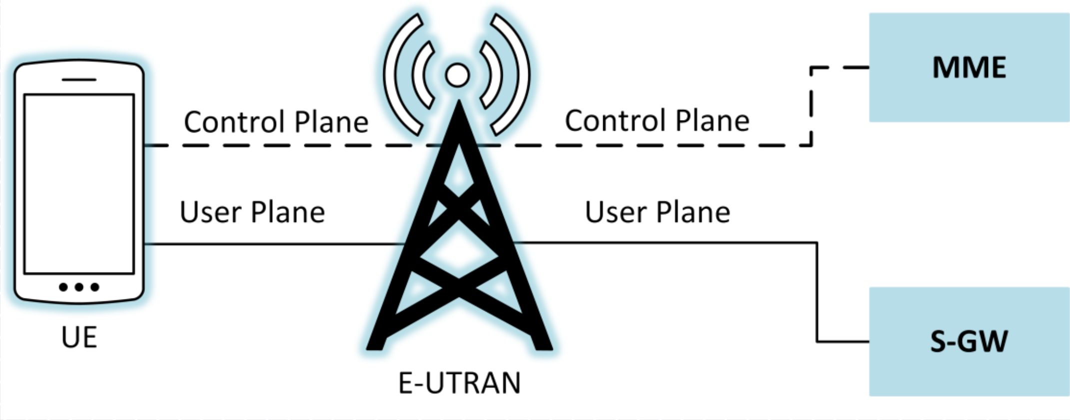
Note: Simplified for brevity

LTE Network


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

Communications Planes

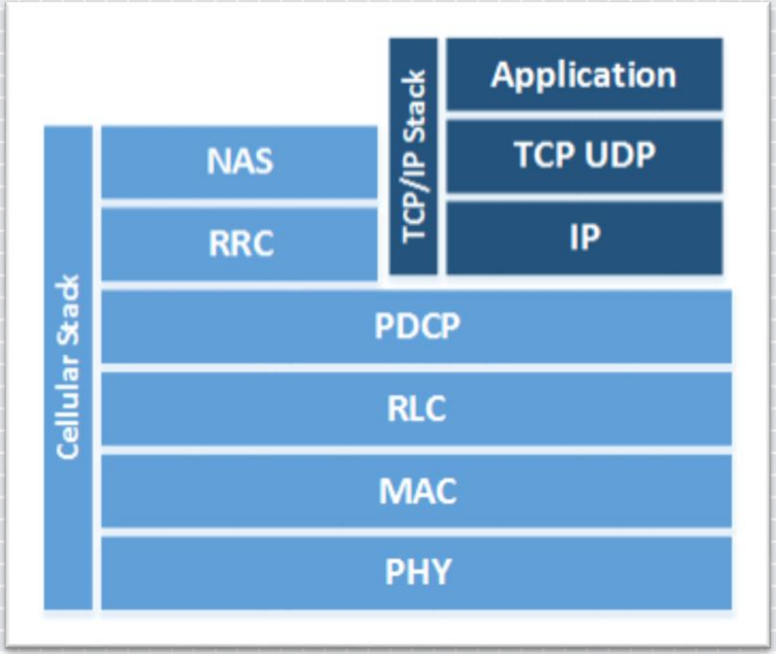
- LTE uses multiple planes of communication
- Different logical planes are multiplexed into same RF signal
- Routed to different end points



LTE Protocols

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

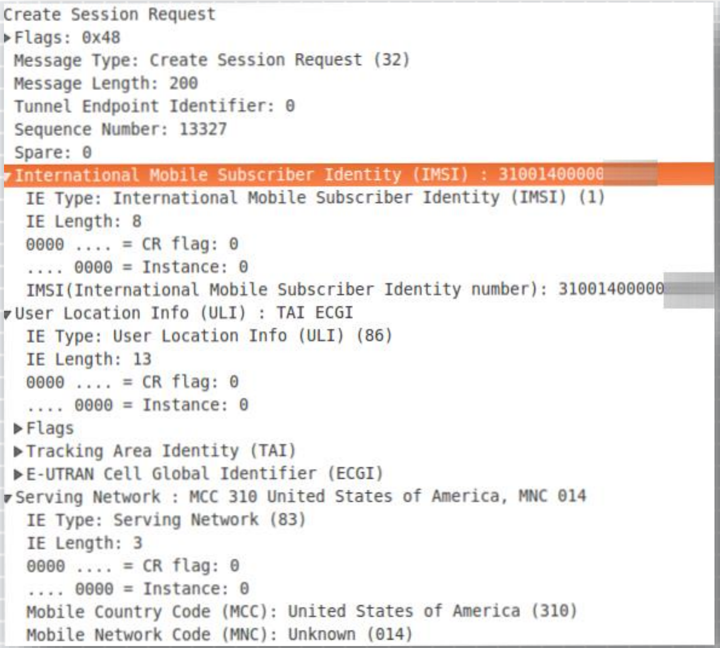
- **Radio Resource Control (RRC):** Transfers NAS messages, AS information may be included, signaling, and ECM
- **Packet Data Convergence Protocol (PDCP):** header compression, radio encryption
- **Radio Link Control (RLC):** Readies packets to be transferred over the air interface
- **Medium Access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



Subscriber Identity (IMSI)

- International Mobile Subscriber Identity (IMSI)
  - LTE uses a unique ID for every subscriber
  - 15 digit number stored on the UICC
  - Consists of 3 values: MCC, MNC, and MSIN
  - Distinct from the subscriber's phone number

MCC	MNC	MSIN
310	014	00000****



```
Create Session Request
▸Flags: 0x48
 Message Type: Create Session Request (32)
 Message Length: 200
 Tunnel Endpoint Identifier: 0
 Sequence Number: 13327
 Spare: 0
▾International Mobile Subscriber Identity (IMSI) : 31001400000
  IE Type: International Mobile Subscriber Identity (IMSI) (1)
  IE Length: 8
  0000 .... = CR flag: 0
  .... 0000 = Instance: 0
  IMSI(International Mobile Subscriber Identity number): 31001400000
▾User Location Info (ULI) : TAI ECGI
  IE Type: User Location Info (ULI) (86)
  IE Length: 13
  0000 .... = CR flag: 0
  .... 0000 = Instance: 0
 ▸Flags
 ▸Tracking Area Identity (TAI)
 ▸E-UTRAN Cell Global Identifier (ECGI)
▾Serving Network : MCC 310 United States of America, MNC 014
  IE Type: Serving Network (83)
  IE Length: 3
  0000 .... = CR flag: 0
  .... 0000 = Instance: 0
  Mobile Country Code (MCC): United States of America (310)
  Mobile Network Code (MNC): Unknown (014)
```

RSAConference2015

San Francisco | April 20-24 | Moscone Center

LTE Security Architecture

#RSAC

LTE Security Architecture

- We will explore several LTE defenses:
  - SIM cards and UICC tokens
  - Device and network authentication
  - Air interface protection (Uu)
  - Backhaul and network protection (S1-MME, S1-U)
- LTE's security architecture is defined by 3GPP's TS 33.401
  - There are many, many, many references to other standards within

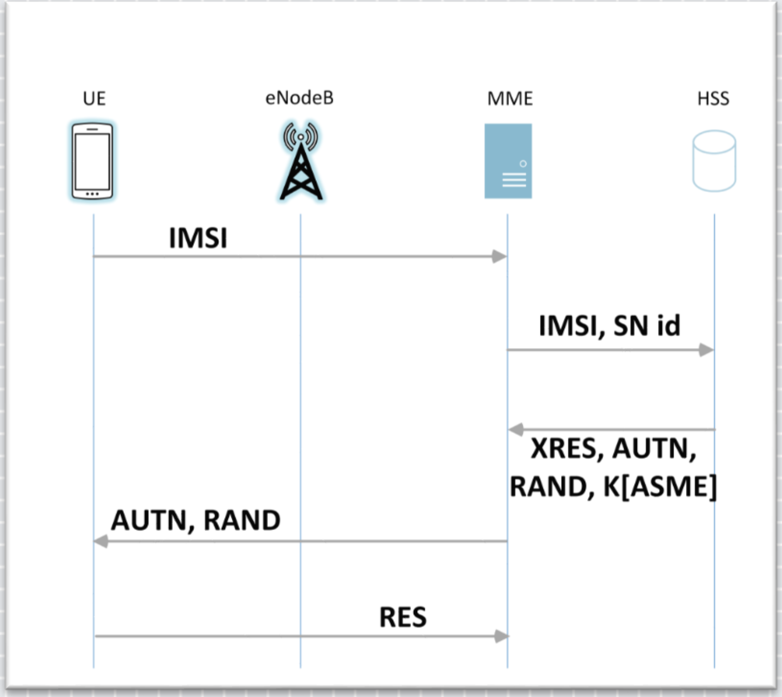
UICC Token

- Hardware storage location for sensitive information
  - Stores pre-shared key K
  - Stores IMSI
- Limited access to the UICC via a restricted API
- Performs cryptographic operations for authentication

TS 33.401 - 6.1.1: Access to E-UTRAN with a 2G SIM or a SIM application on a UICC shall not be granted.

Device & Network Authentication

- Authentication and Key Agreement (AKA) is the protocol used for devices to authenticate with the carrier to gain network access
- The cryptographic keys needed to encrypt calls are generated upon completion of the AKA protocol



3GPP 33.401 - 6.1.1: EPS AKA is the authentication and key agreement procedure that shall be used over E-UTRAN.

AKA Packet Capture

Sending Temporary Identity

```
NAS-PDU: 17a402ae6a030741510bf6134010100001c0400a1e02e0e0...
▼Non-Access-Stratum (NAS)PDU
  0001 .... = Security header type: Integrity protected (1)
  .... 0111 = Protocol discriminator: EPS mobility management messages (0x
  Message authentication code: 0xa402ae6a
  Sequence number: 3
  0000 .... = Security header type: Plain NAS message, not security protec
  .... 0111 = Protocol discriminator: EPS mobility management messages (0x
  NAS EPS Mobility Management Message Type: Attach request (0x41)
  0... .... = Type of security context flag (TSC): Native security context
  .101 .... = NAS key set identifier:  (5)
  .... 0... = Spare bit(s): 0x00
  .... .001 = EPS attach type: EPS attach (1)
 ▼EPS mobile identity
   Length: 11
   .... 0... = odd/even indic: 0
   .... .110 = Type of identity: GUTI (6)
   Mobile Country Code (MCC): United States of America (310)
   Mobile Network Code (MNC): Unknown (014)
   MME Group ID: 4096
   MME Code: 1
   M-TMSI: 0xc0400a1e
 ▶UE network capability
 ▶ESM message container
 ▶Tracking area identity - Last visited registered TAI
▼Item 2: id-TAI
 ▼ProtocolIE-Field
   id: id-TAI (67)
   criticality: reject (0)
  ▼value
```

Authentication Vectors

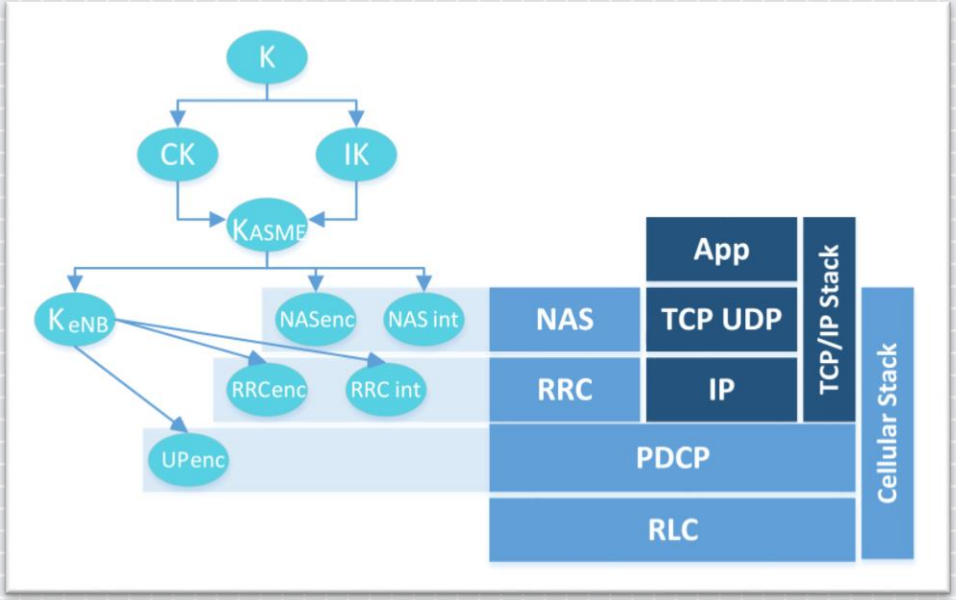
```
   id: id-eNB-UE-S1AP-ID (8)
   criticality: reject (0)
  ▼value
    ENB-UE-S1AP-ID: 15
▼Item 2: id-NAS-PDU
 ▼ProtocolIE-Field
   id: id-NAS-PDU (26)
   criticality: reject (0)
  ▼value
    NAS-PDU: 075206fbd8d1e49c99d71590d2f0562bc10430109c3c575a...
   ▼Non-Access-Stratum (NAS)PDU
     0000 .... = Security header type: Plain NAS message, not security protected (0)
     .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
     NAS EPS Mobility Management Message Type: Authentication request (0x52)
     0000 .... = Spare half octet: 0
     .... 0... = Type of security context flag (TSC): Native security context (for KSIasme)
     .... .110 = NAS key set identifier:  (6) ASME
    ▼Authentication Parameter RAND - EPS challenge
      RAND value: fbd8d1e49c99d71590d2f0562bc10430
    ▼Authentication Parameter AUTN (UMTS and EPS authentication challenge) - EPS challenge
      Length: 16
     ▼AUTN value: 9c3c575aebb3800022615f8b19912203
       SQN xor AK: 9c3c575aebb3
       AMF: 8000
       MAC: 22615f8b19912203
```

Authentication Response

```
     .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
     Message authentication code: 0x9a00d54c
     Sequence number: 4
     0000 .... = Security header type: Plain NAS message, not security protected (0)
     .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
     NAS EPS Mobility Management Message Type: Authentication response (0x53)
    ▼Authentication response parameter
      Length: 8
      RES: 7dbfefe9561e7b08
▶Item 3: id-EUTRAN-CGI
▼Item 4: id-TAI
 ▼ProtocolIE-Field
   id: id-TAI (67)
   criticality: ignore (1)
  ▼value
   ▼TAI
     pLMNidentity:
     Mobile Country Code (MCC): United States of America (310)
     Mobile Network Code (MNC): Unknown (014)
     tAC:
```

Cryptographic Key Usage

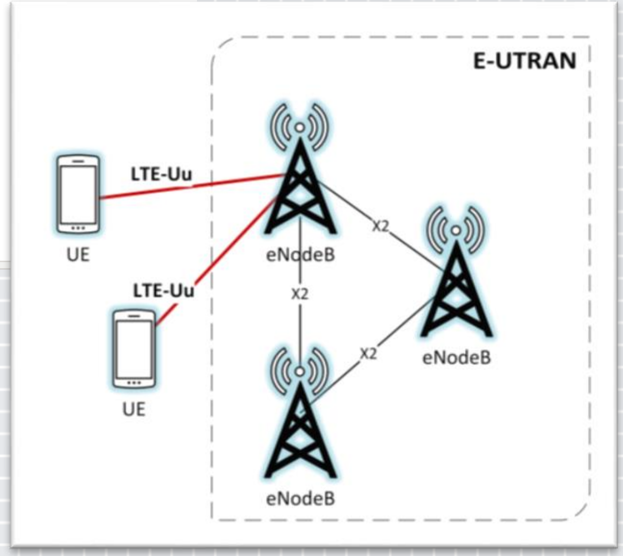
- **K**: 128-bit master key. Put into USIM and HSS by carrier
- **CK & IK**: 128-bit Cipher key and Integrity key
- **KASME** : 256-bit local master, derived from CK & IK
- **KeNB**: 256-bit key used to derive additional keys
- **NASenc & NASint**: 256/128-bit key protecting NAS
- **RRCenc & RRCint**: 256/128-bit key protecting RRC
- **UPenc:** 256/128-bit key protecting UP traffic



Air Interface Protection

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

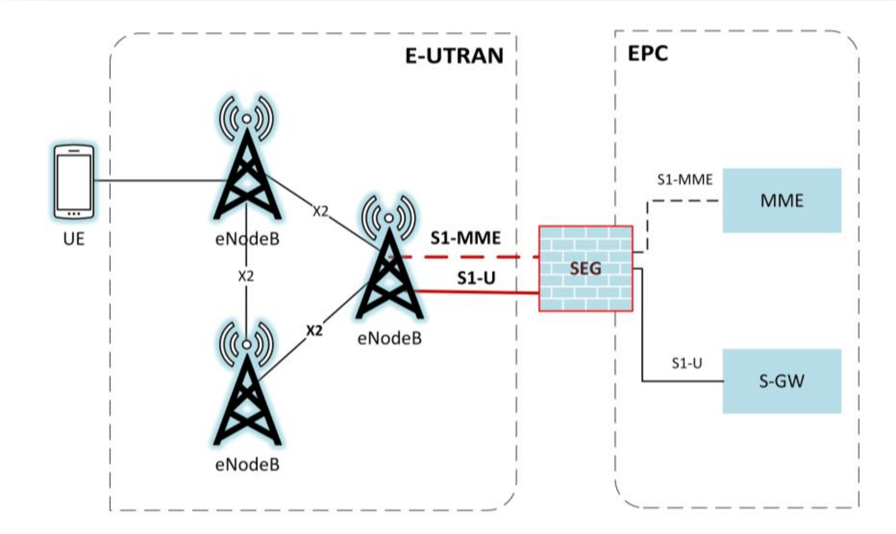
```
▼UE security capability - Replayed UE security capabilities
  Length: 2
  1... .... = EEA0: Supported
  .1.. .... = 128-EEA1: Supported
  ..1. .... = 128-EEA2: Supported
  ...0 .... = 128-EEA3: Not Supported
  .... 0... = EEA4: Not Supported
  .... .0.. = EEA5: Not Supported
  .... ..0. = EEA6: Not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



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

Backhaul Protection

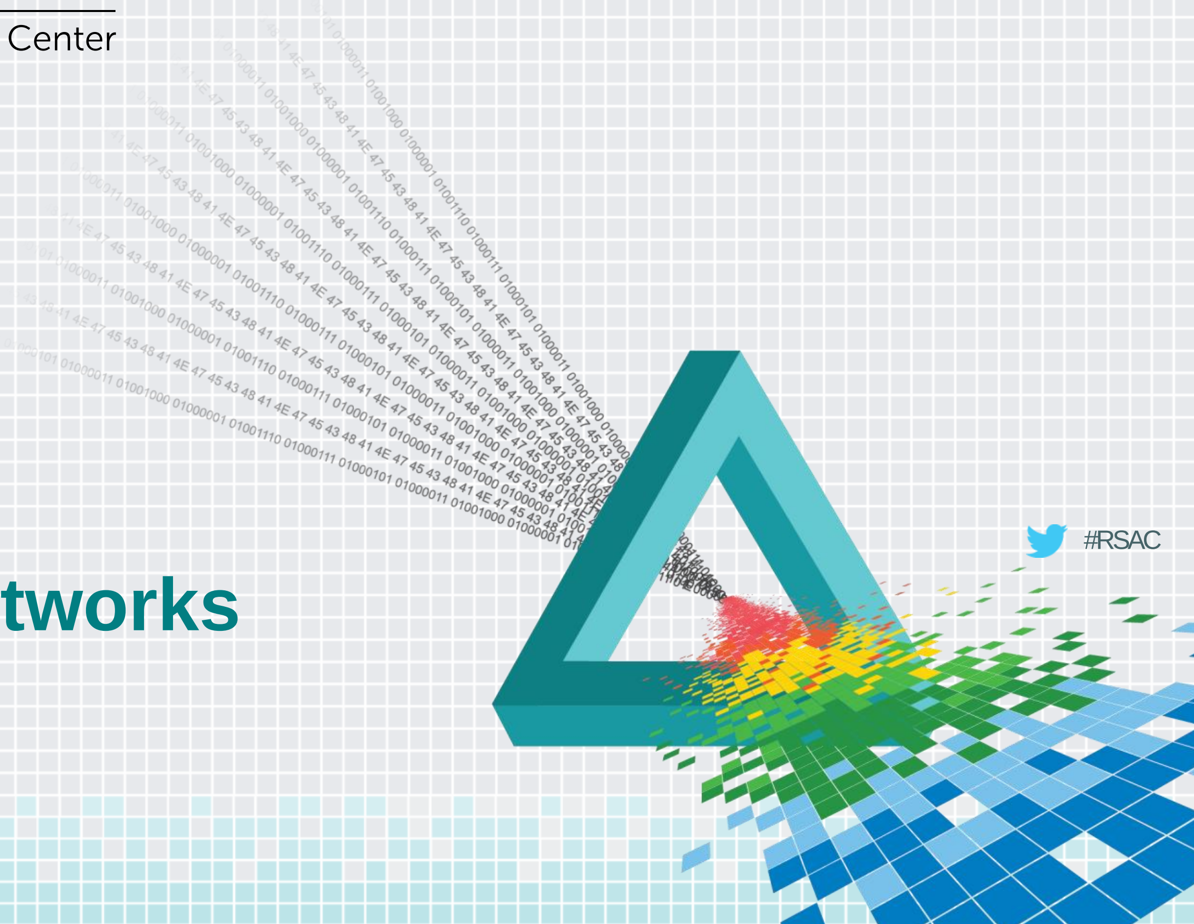
- Confidentiality protection of traffic running over S1 Interface (Backhaul)
- Hardware security appliances are used to implement this standard
- Security Gateways (SEG)
- IPSEC tunnel created between eNodeB and SEG



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

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

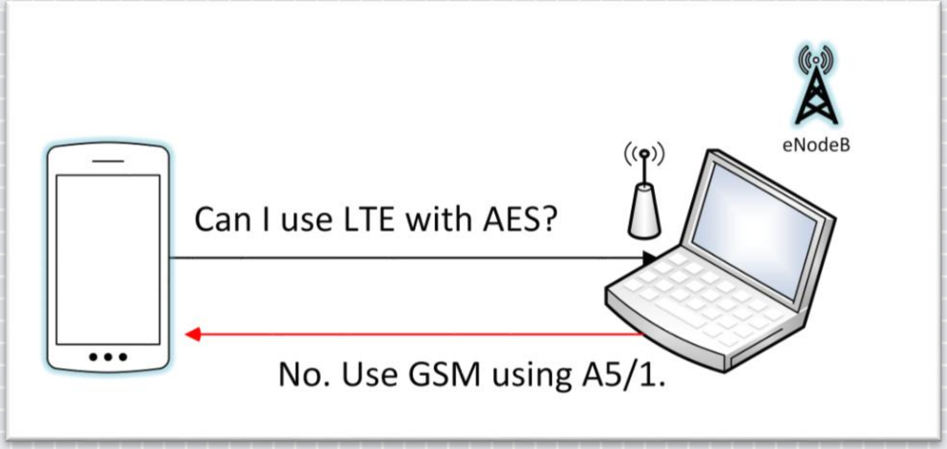
Threats to LTE Networks

General Computer Security Threats

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

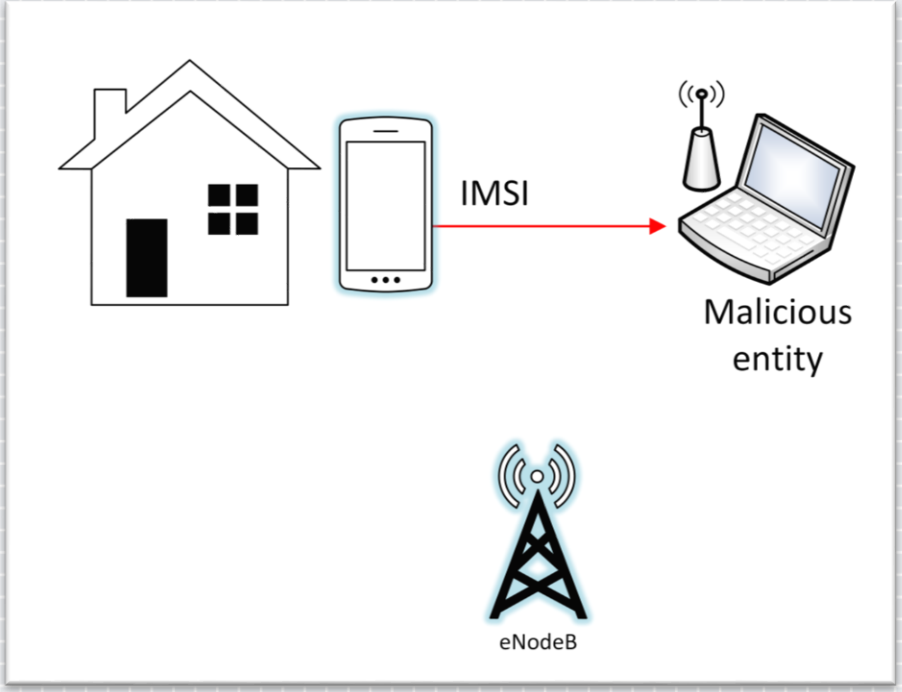
Renegotiation Attacks

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



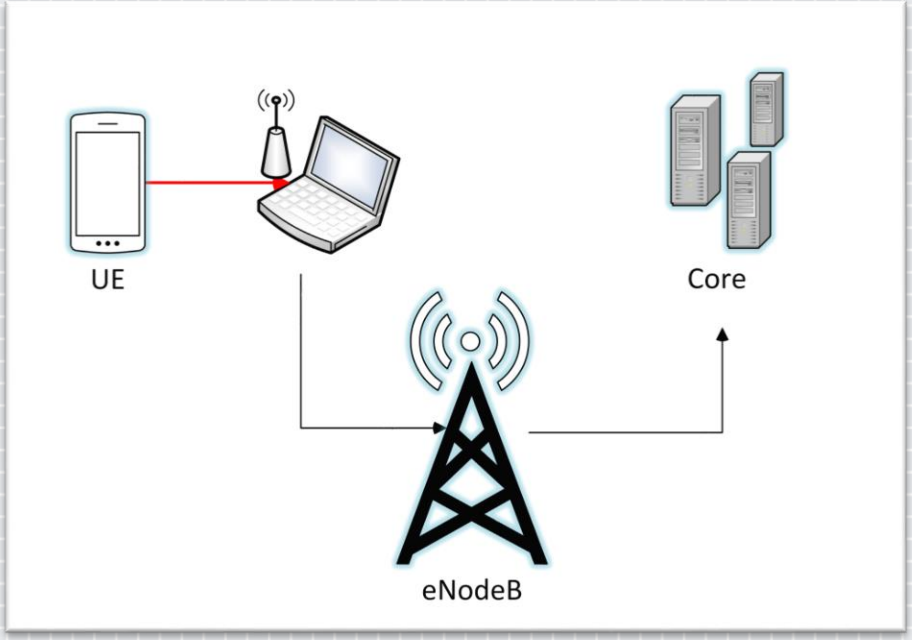
Device & Identity Tracking

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



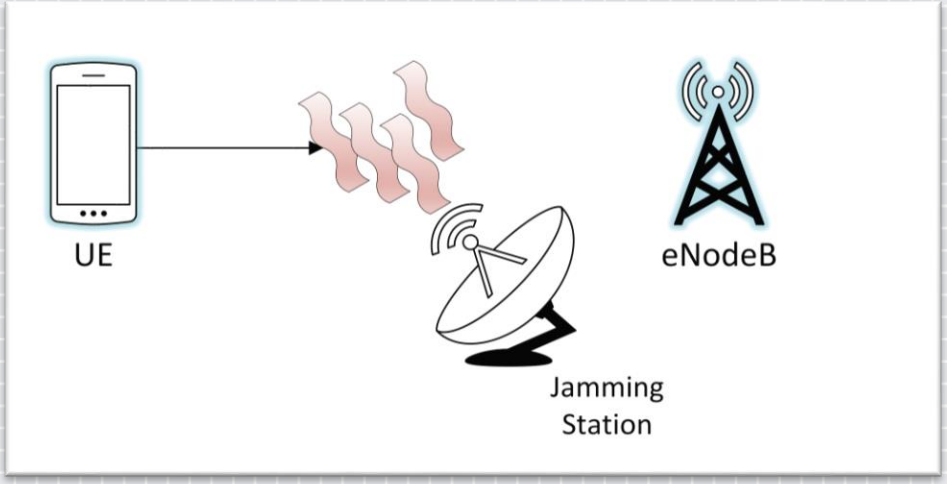
Call Interception

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



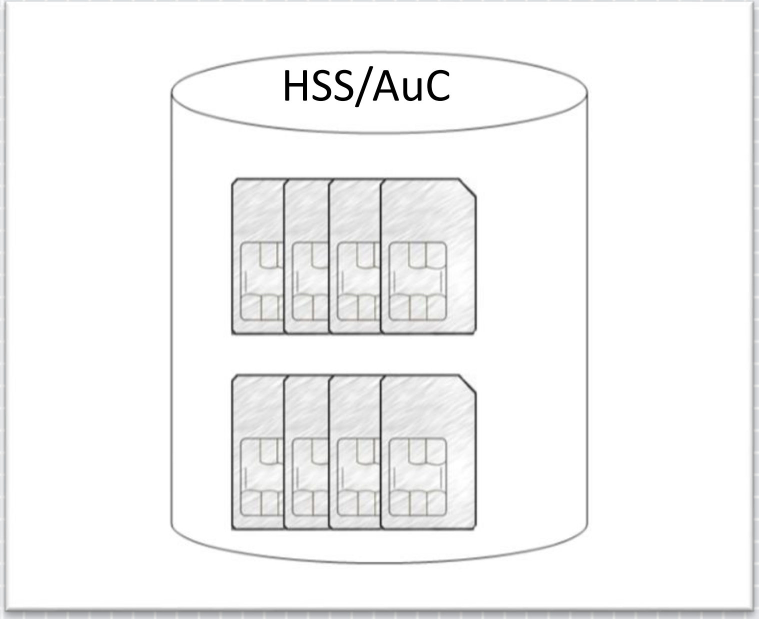
Jamming UE Radio Interface

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



Attacks Against the Secret Key (K)

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

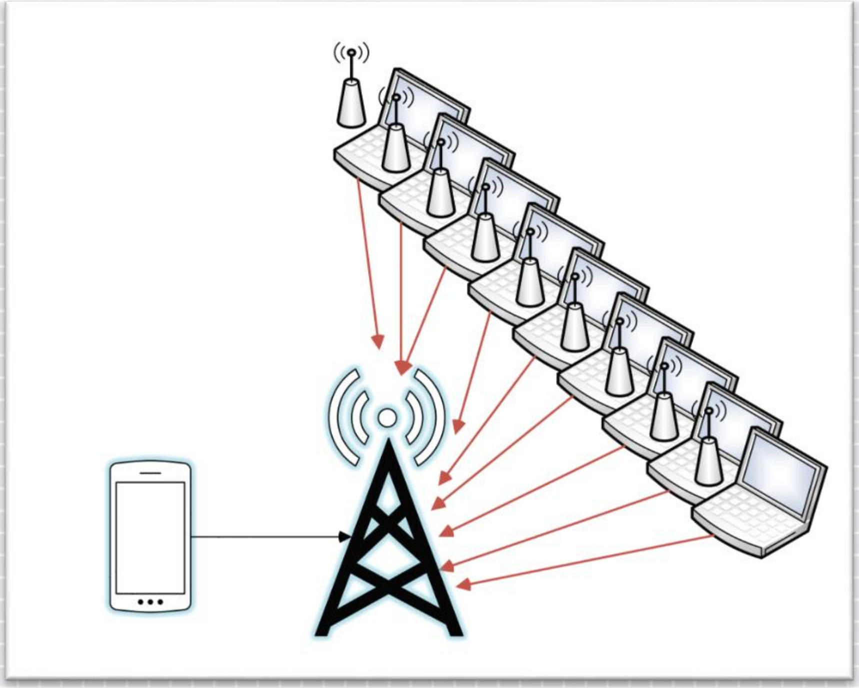


Physical Base Station Attacks

- **Threat:** The radio equipment and other electronics required to operate a base station may be physically destroyed
- **Mitigation:** Provide adequate physical security measures such as video surveillance, gates, and various tamper detection mechanisms

Availability Attacks on eNodeB & Core

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



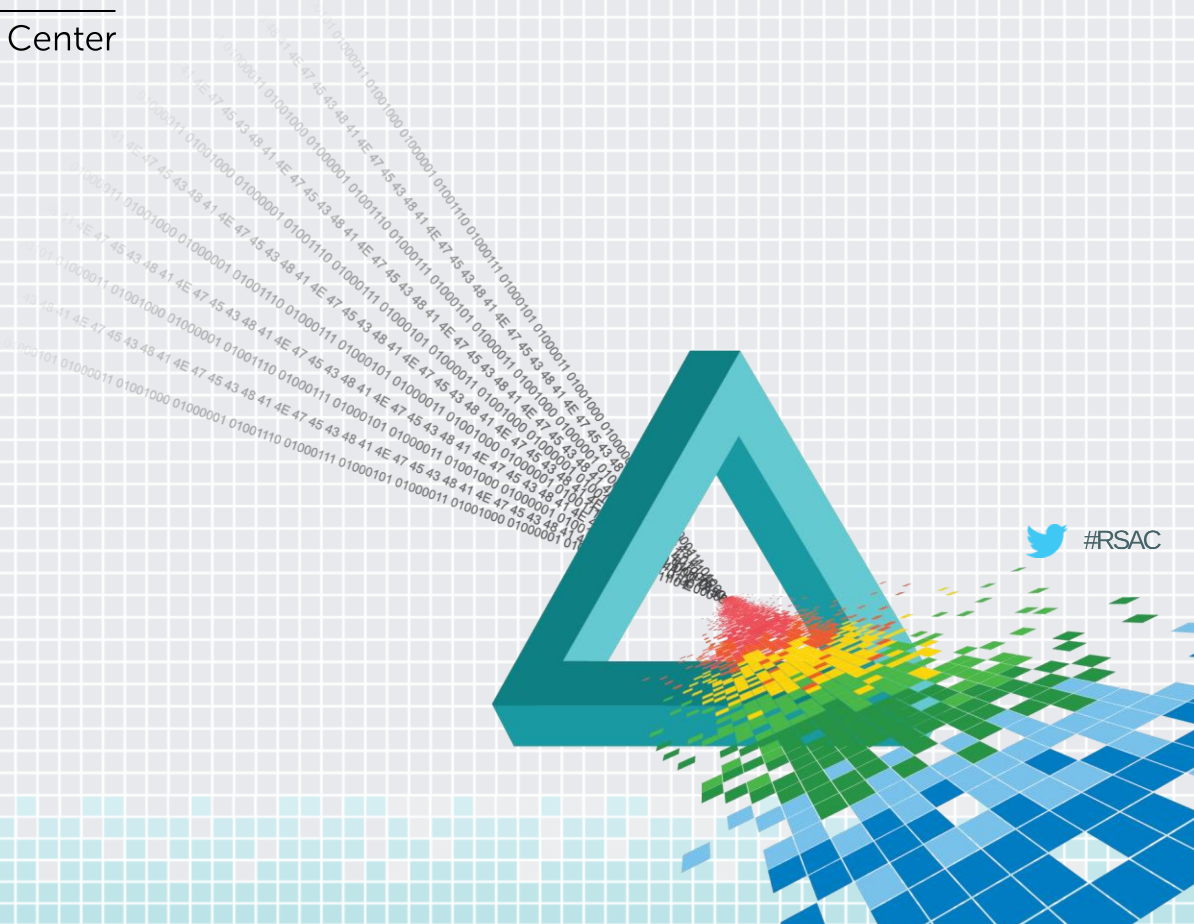
Apply What You Learned Today

- Following this talk:
  - Take notice when you're connected to non-LTE networks (e.g., EDGE, GPRS, UMTS, HSPA, WiFi)
  - Understand protections are offered by LTE – and what isn't
- Don't send sensitive information over untrusted or non-LTE networks
  - LTE helps mitigate rogue base station attacks

Summary – How Good is it?

- LTE security is markedly more secure than its predecessors
- Strong security mechanisms are baked-in
  - Unfortunately, many of them are optional or may not be on by default
  - Although integrity protection mechanisms are required
  - Call your friendly neighborhood wireless carrier today
- Unaddressed threats exist (e.g., *jamming*)
  - Some are outside the purview of the carriers & standards bodies, such as SoC manufacturers
- LTE is always evolving
  - Today's defenses are not etched in stone
  - Upgrades are in the works via 3GPP Working Groups

Questions?



#RSAC

Selected Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
AuC	Authentication Center
AS	Access Stratum
AUTN	Authentication token
CP	Control Plane
EDGE	Enhanced Data Rates for GSM Evolution
eNB	eNodeB, Evolved Node B
eNodeBEvolved Node B	
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary UE Identity
HSS	Home Subscriber Server
IMEI	International Mobile Equipment Identifier
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
K	Secret Key K
LTE	Long Term Evolution
ME	Mobile Equipment
MME	Mobility Management Entity
NAS	Network Access Stratum
NIST	National Institute of Standards & Technology
PDCP	Packet Data Convergence Protocol
P-GW	Packet Gateway
PHY	Physical
PSCR	Public Safety Communications Research
RAND	Random
RES	Response
RLC	Radio Link Control
RRC	Radio Resource Control
S-GW	Serving Gateway
SQN	Sequence Number
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
XRES	Expected result

References

- 3GPP TS 33.102: “3G security; Security architecture”
- 3GPP TS 22.101: “Service aspects; Service principles”
- 3GPP TS 33.210: “3G security; Network Domain Security (NDS); IP network layer security”
- 3GPP TS 33.401: “3GPP System Architecture Evolution (SAE); Security architecture”
- 3GPP TR 33.821: “Rationale and track of security decisions in LTE”
- D. Forsberg, G.Horn, W.-D. Moeller, and V. Niemi, *LTE Security*, 2nd ed., John Wiley & Sons, Ltd.: United Kingdom, 2012.
- Pico, Parez, Attacking 3G, Rooted 2014.
- Prasad, Anand, 3GPP SAE/LTE Security, NIKSUN WWSMC, 2011.
- Schneider, Peter, “How to secure an LTE-network: Just applying the 3GPP security standards and that's it?”, Nokia, 2012.