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

LTE Security – How Good Is It?

Michael Bartock
IT Specialist (Security)
National Institute of Standards & Technology

Jeffrey Cichonski
IT Specialist (Security)
National Institute of Standards & Technology

Joshua Franklin
IT Specialist (Security)
National Institute of Standards & Technology

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.

Agenda

- Discussion of LTE standards
- Description of LTE technology
- Exploration of LTE's protection mechanisms
  - In-depth discussion of applied backhaul security research
- 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

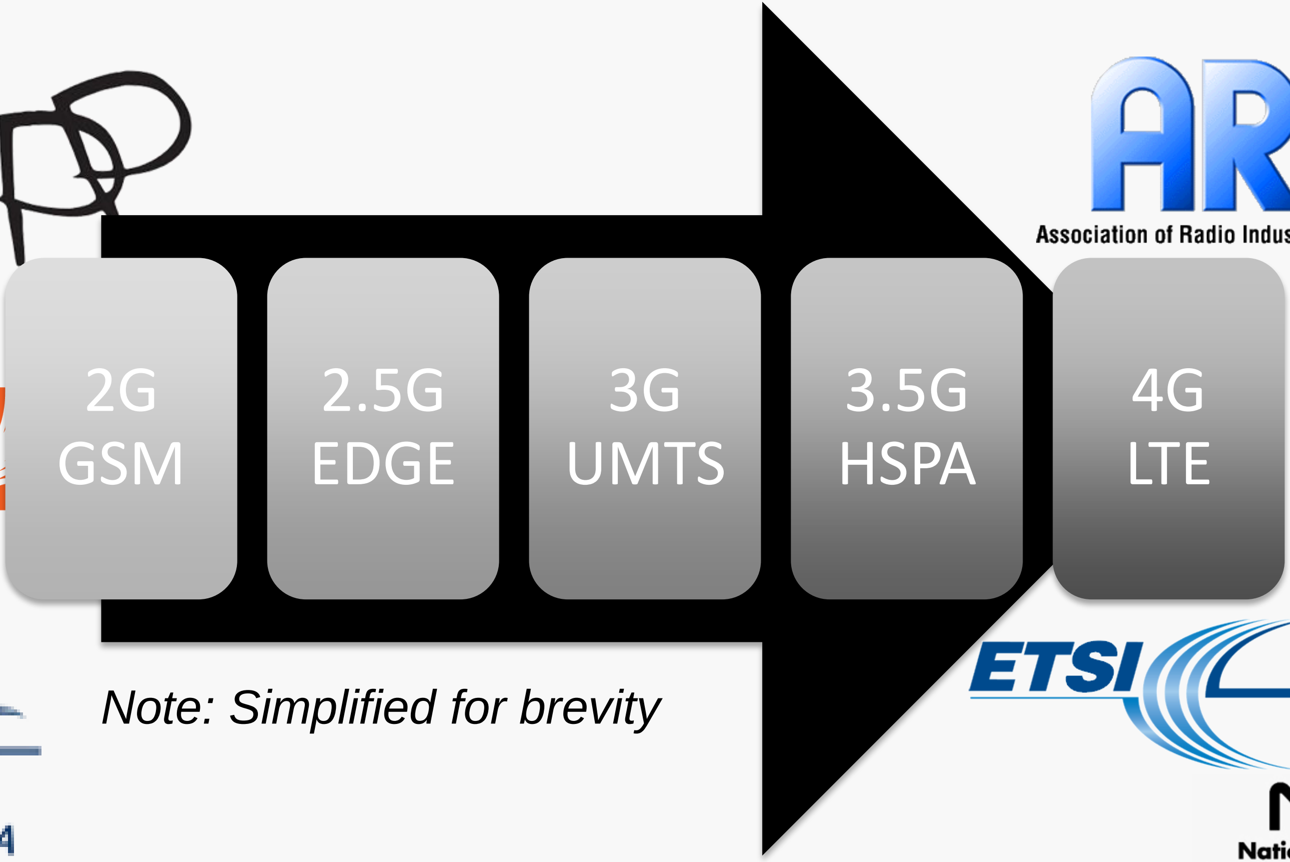
Cybersecurity Research Objectives

- Led by the Information Technology Laboratory's Computer Security Division with support from Software and System Division and Information Access Division
- Kicked off at the PSCR stakeholder meeting in June 2013
- Takes a holistic approach to cybersecurity for public safety communications
- Leverages existing mobile cybersecurity efforts within the government and industry
- Conduct research to fill gaps in cybersecurity

Cybersecurity Research Objectives

- LTE architecture, standards, and security (NISTIR)
- Identity management for public safety (NISTIR 8014)
- Mobile application security for public safety
- Enabling cybersecurity features in the PSCR demonstration network
- Mapping public safety communication network requirements to standard cybersecurity controls and frameworks (NISTIR)
- Usable cybersecurity for public safety

3GPP Standards & Evolution



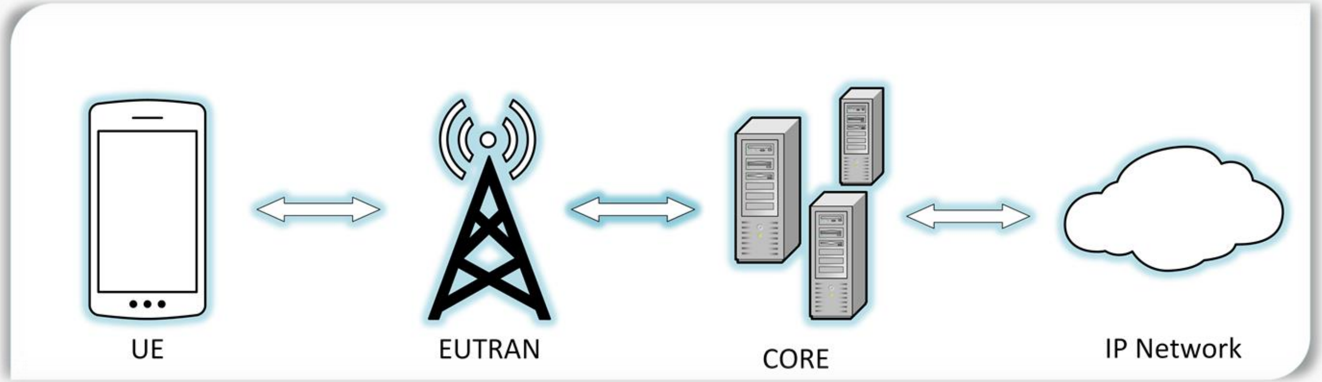
Note: Simplified for brevity

LTE Technology Overview

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

The Basics

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



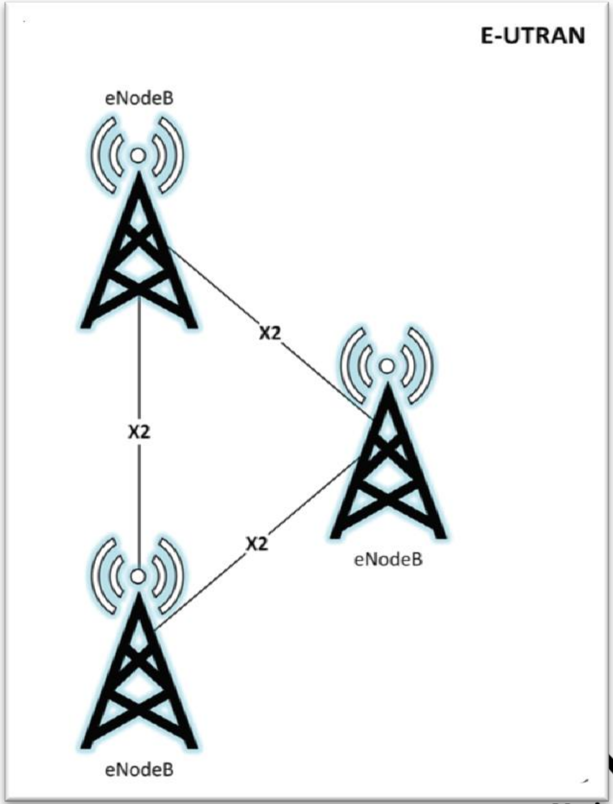
National Institute of Standards and Technology
U.S. Department of Commerce

Mobile Device

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

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

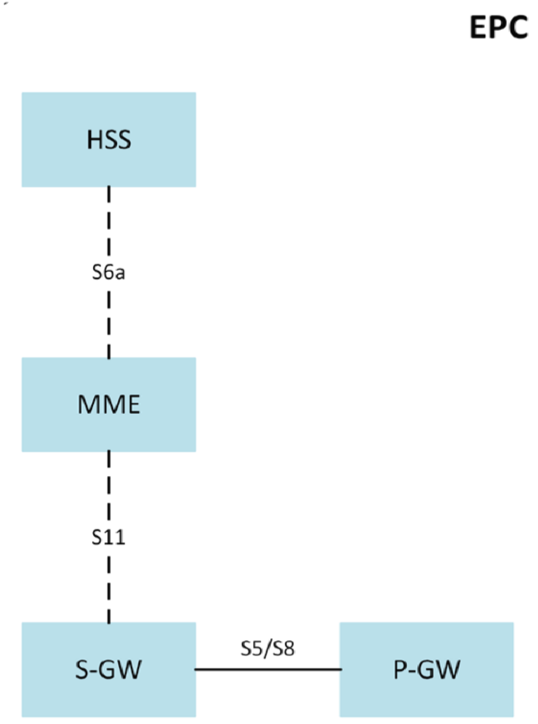
- **eNodeB:** Radio component of LTE network
  - De-modulates RF signals & transmits IP packets to core network
  - Modulates IP packets & transmits RF signals to UE
- **E-UTRAN:** mesh network of eNodeBs
- **X2 Interface:** connection between eNodeBs



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

Evolved Packet Core (EPC)

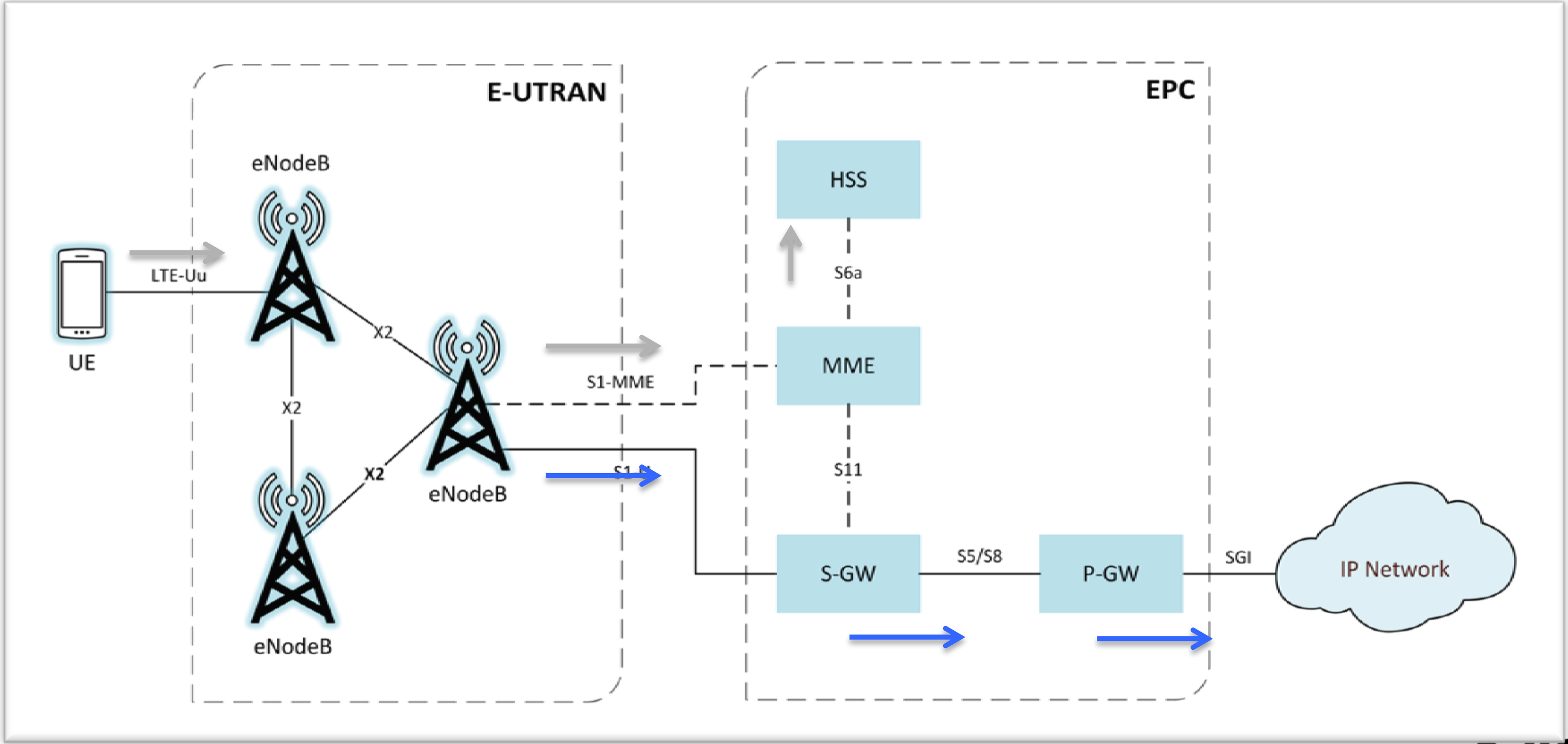
- **Mobility Management Entity (MME)**
  - Primary signaling node - does not interact with user traffic
  - Functions include managing & storing UE contexts, creating temporary IDs, sending pages, controlling authentication functions, & selecting the S-GW and P-GWs
- **Serving Gateway (S-GW)**
  - Router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



Note: Simplified for brevity

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

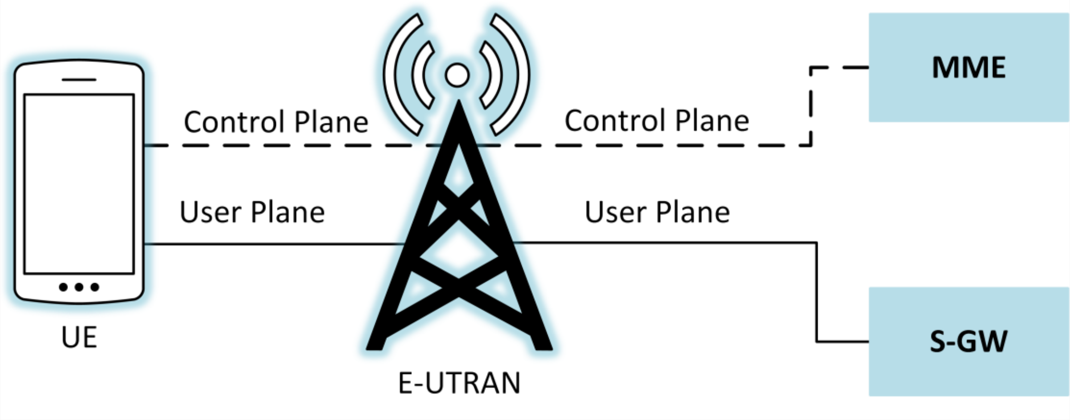
LTE Network



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

Communications Planes

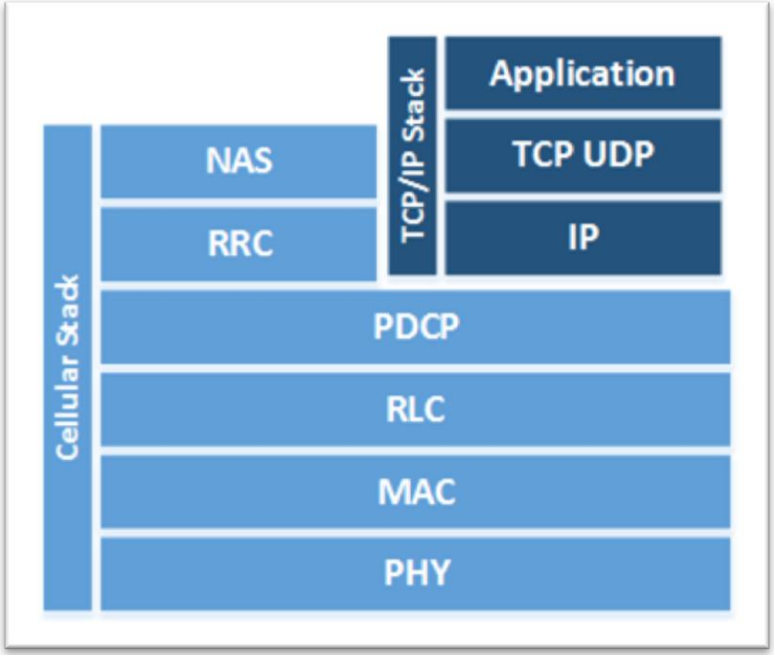
- LTE uses multiple planes of communication
- Different logical planes are multiplexed into same RF signal
- Routed to different end points



LTE Protocols

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

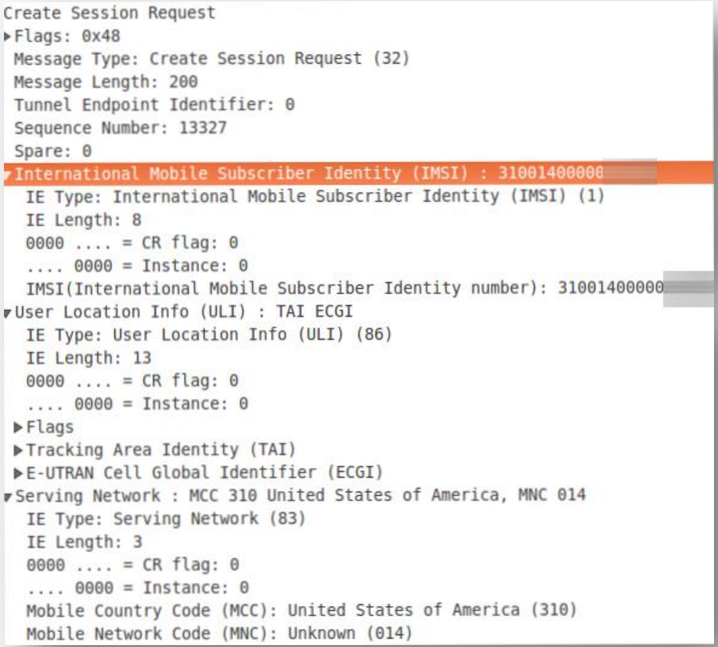
- **Radio Resource Control (RRC):** Transfers NAS messages, AS information may be included, signaling, and ECM
- **Packet Data Convergence Protocol (PDCP):** header compression, radio encryption
- **Radio Link Control (RLC):** Readies packets to be transferred over the air interface
- **Medium Access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



LTE Security Architecture

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

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

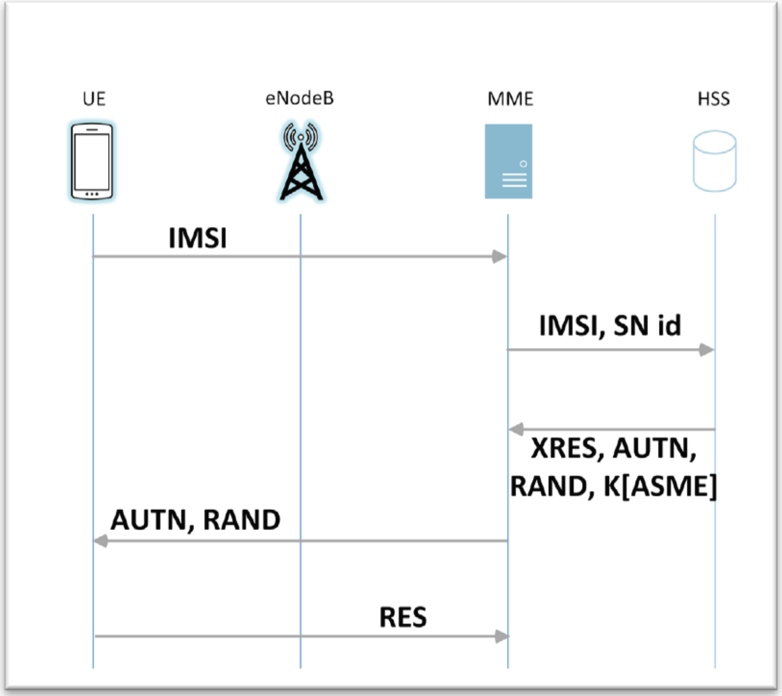
- Hardware storage location for sensitive information
  - Stores pre-shared key K
  - Stores IMSI
- Limited access to the UICC via a restricted API
- Performs cryptographic operations for authentication

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.

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

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.

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

AKA Packet Capture

Sending Temporary Identity

```
NAS-PDU: 17a402ae6a0307415106f6134010100001c0400a1e02e0e0...
▼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
```

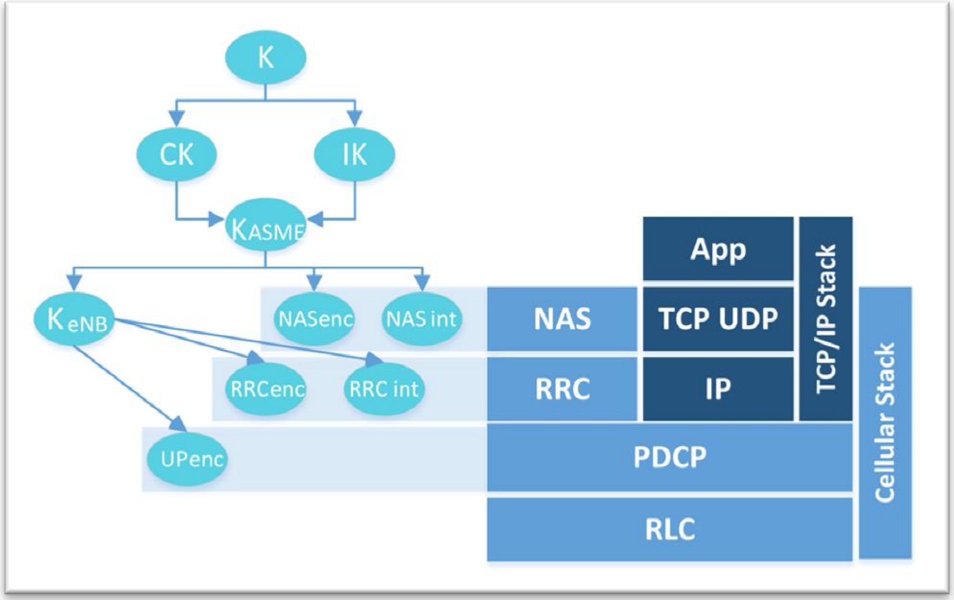
Authentication Response

```
  .... 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:
```

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

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

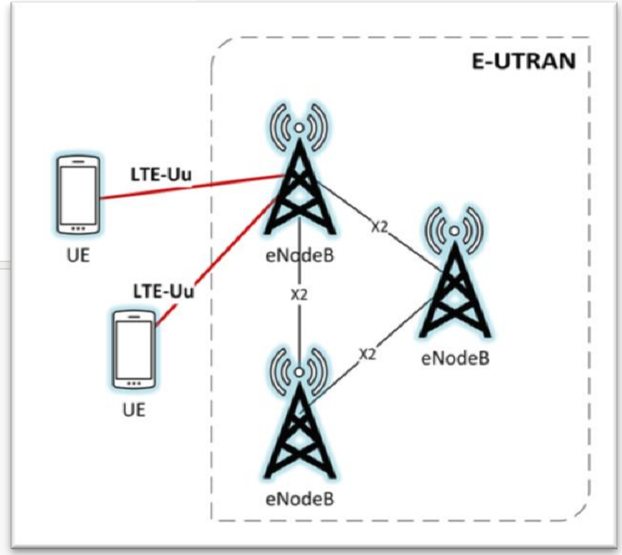


National Institute of Standards and Technology
U.S. Department of Commerce

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
```

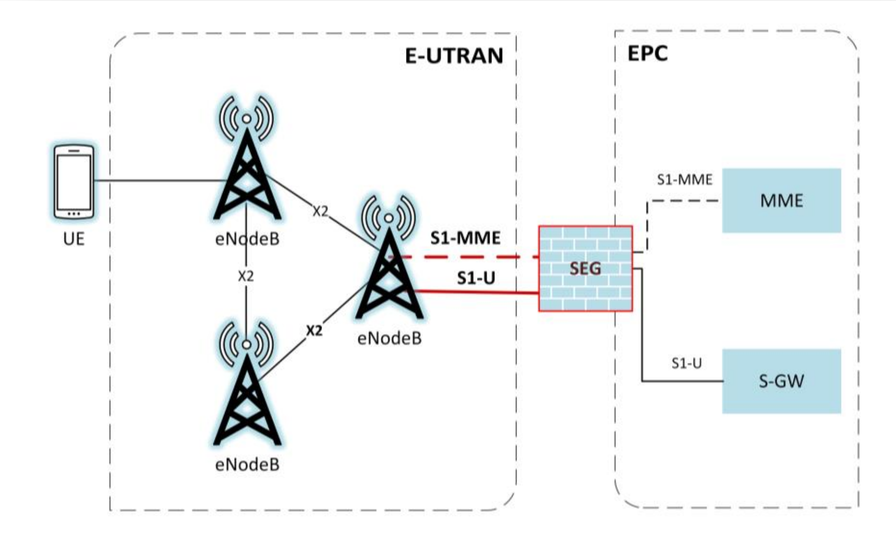


3GPP 33.401- 5.1.3.1: User plane confidentiality protection shall be done at PDCP layer and is an operator option.

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

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.

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

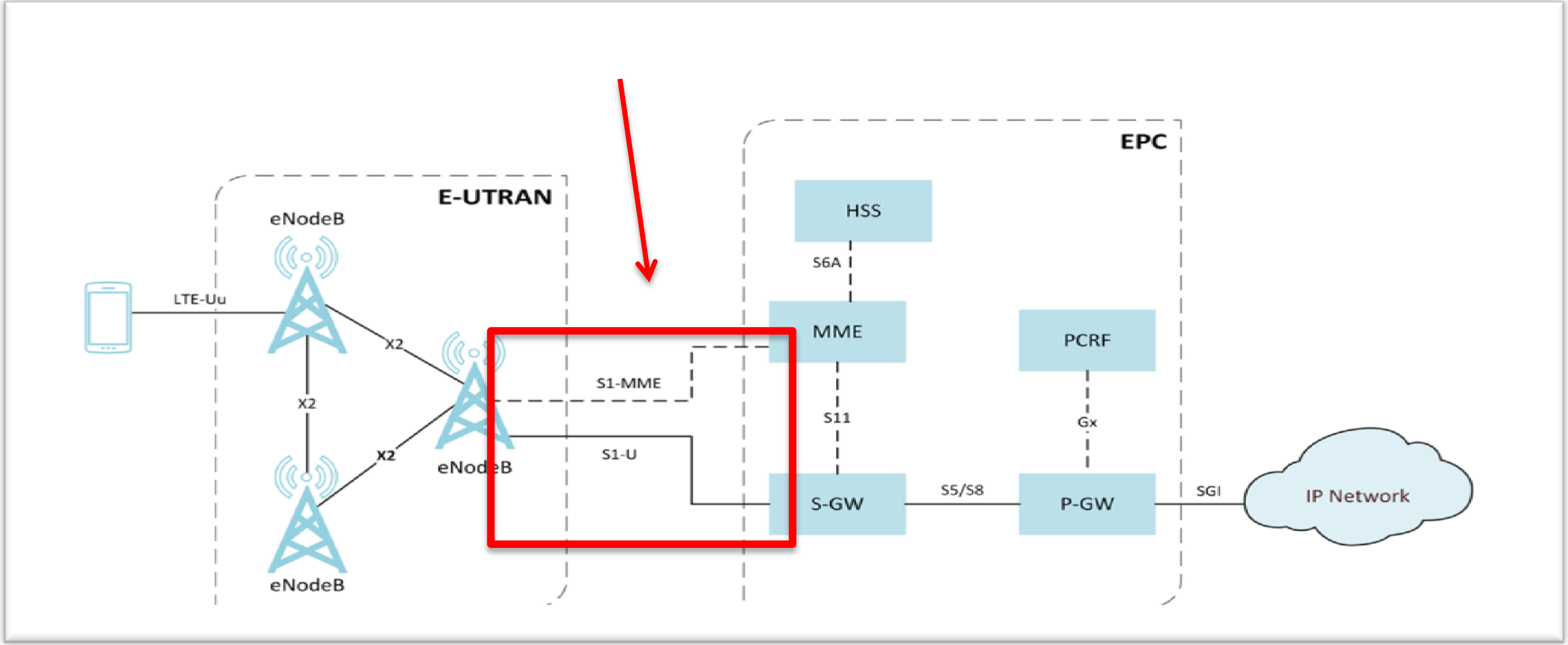
PSCR Applied Research

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

PSCR Applied Research

- Our Focus is on communication from the cell site to core network.

Our Focus is on communication from the cell site to core network.



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

Initial Research Goal

- Enable data encryption on the backhaul connection.
- Verify data is encrypted.
- Analyze impact on networks performance.
- Encourage the default use of backhaul encryption.

Why Encrypt the Backhaul

- User data travels over the backhaul.
- The backhaul may or may not be trusted.
  - Example: Operator A uses Operators B’s fiber trunk to connect remote cell sites to its core network.
- An adversary could be listening in on this connection.

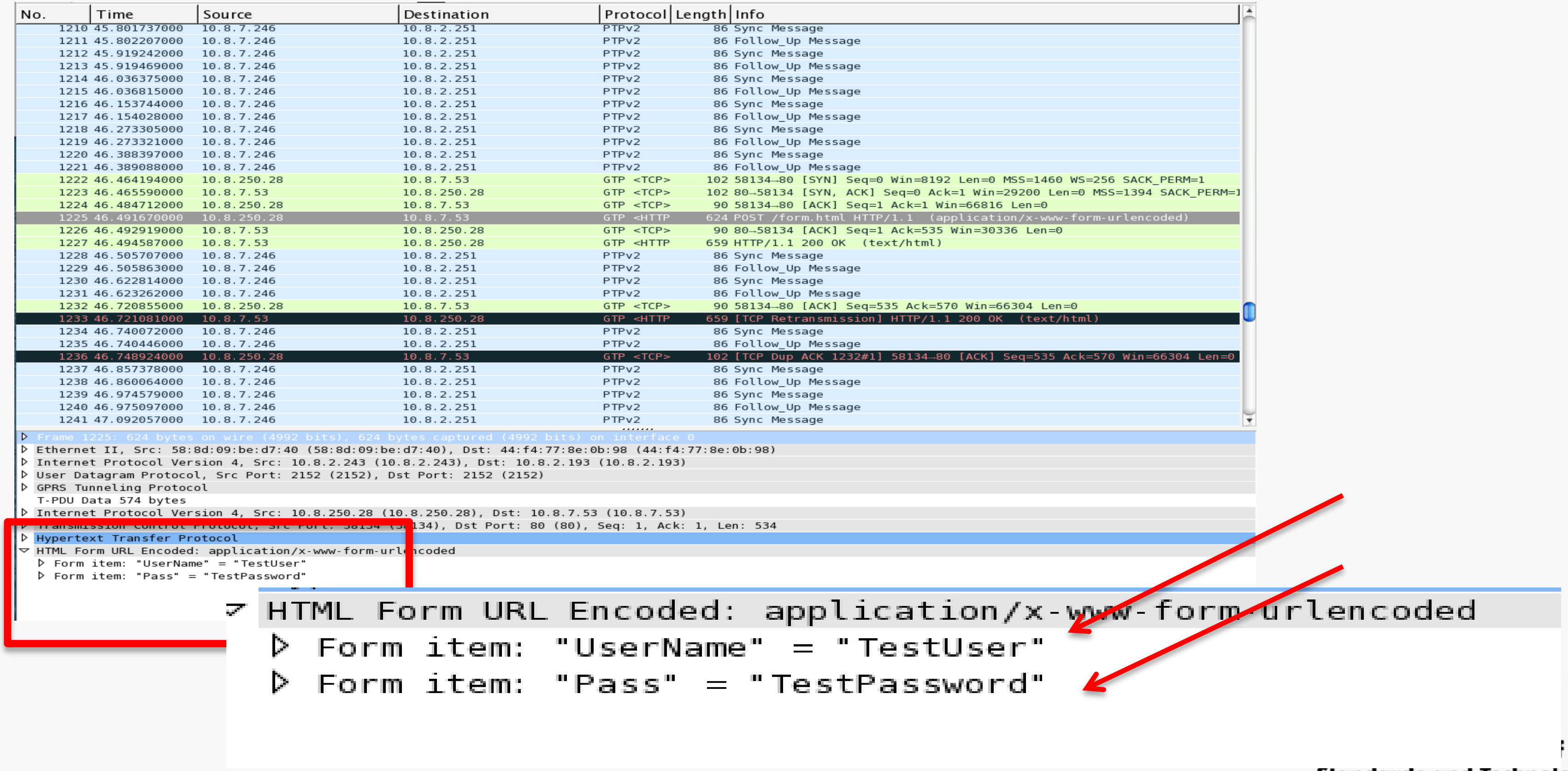
Implementation

- Use Internet Protocol Security **(IPSEC)** to encrypt this communication.
  - Provides encryption at the Internet layer of the IP protocol stack
  - Commercial base stations support IPSEC
- Use public key infrastructure (PKI) certificates to provide strong authentication.
  - Base station and core network authenticate each other.

Current State of Research

- Collaborating with CRADA partners to identify commercial grade solutions
- Implemented backhaul protection on part of PSCR Demonstration Network
- Testing impacts on network performance
- Working to verify interoperability & scalability

Non Encrypted Traffic



No.	Time	Source	Destination	Protocol	Length	Info
1210	45.801737000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1211	45.802207000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1212	45.919242000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1213	45.919469000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1214	46.036375000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1215	46.036815000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1216	46.153744000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1217	46.154028000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1218	46.273305000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1219	46.273321000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1220	46.388397000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1221	46.389088000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1222	46.464194000	10.8.250.28	10.8.7.53	GTP <TCP>	102	58134→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1223	46.465590000	10.8.7.53	10.8.250.28	GTP <TCP>	102	80→58134 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1394 SACK_PERM=1
1224	46.484712000	10.8.250.28	10.8.7.53	GTP <TCP>	90	58134→80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
1225	46.491670000	10.8.250.28	10.8.7.53	GTP <HTTP	624	POST /form.html HTTP/1.1 (application/x-www-form-urlencoded)
1226	46.492919000	10.8.7.53	10.8.250.28	GTP <TCP>	90	80→58134 [ACK] Seq=1 Ack=535 Win=30336 Len=0
1227	46.494587000	10.8.7.53	10.8.250.28	GTP <HTTP	659	HTTP/1.1 200 OK (text/html)
1228	46.505707000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1229	46.505863000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1230	46.622814000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1231	46.623262000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1232	46.720855000	10.8.250.28	10.8.7.53	GTP <TCP>	90	58134→80 [ACK] Seq=535 Ack=570 Win=66304 Len=0
1233	46.721081000	10.8.7.53	10.8.250.28	GTP <HTTP	659	[TCP Retransmission] HTTP/1.1 200 OK (text/html)
1234	46.740072000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1235	46.740446000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1236	46.748924000	10.8.250.28	10.8.7.53	GTP <TCP>	102	[TCP Dup ACK 1232#1] 58134→80 [ACK] Seq=535 Ack=570 Win=66304 Len=0
1237	46.857378000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1238	46.860064000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1239	46.974579000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message
1240	46.975097000	10.8.7.246	10.8.2.251	PTPv2	86	Follow_Up Message
1241	47.092057000	10.8.7.246	10.8.2.251	PTPv2	86	Sync Message

Frame 1225: 624 bytes on wire (4992 bits), 624 bytes captured (4992 bits) on interface 0
Ethernet II, Src: 58:8d:09:be:d7:40 (58:8d:09:be:d7:40), Dst: 44:f4:77:8e:0b:98 (44:f4:77:8e:0b:98)
Internet Protocol Version 4, Src: 10.8.2.243 (10.8.2.243), Dst: 10.8.2.193 (10.8.2.193)
User Datagram Protocol, Src Port: 2152 (2152), Dst Port: 2152 (2152)
GPRS Tunneling Protocol
T-PDU Data 574 bytes
Internet Protocol Version 4, Src: 10.8.250.28 (10.8.250.28), Dst: 10.8.7.53 (10.8.7.53)
Transmission Control Protocol, Src Port: 58134 (58134), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 534
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "UserName" = "TestUser"
Form item: "Pass" = "TestPassword"

HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "UserName" = "TestUser"
Form item: "Pass" = "TestPassword"

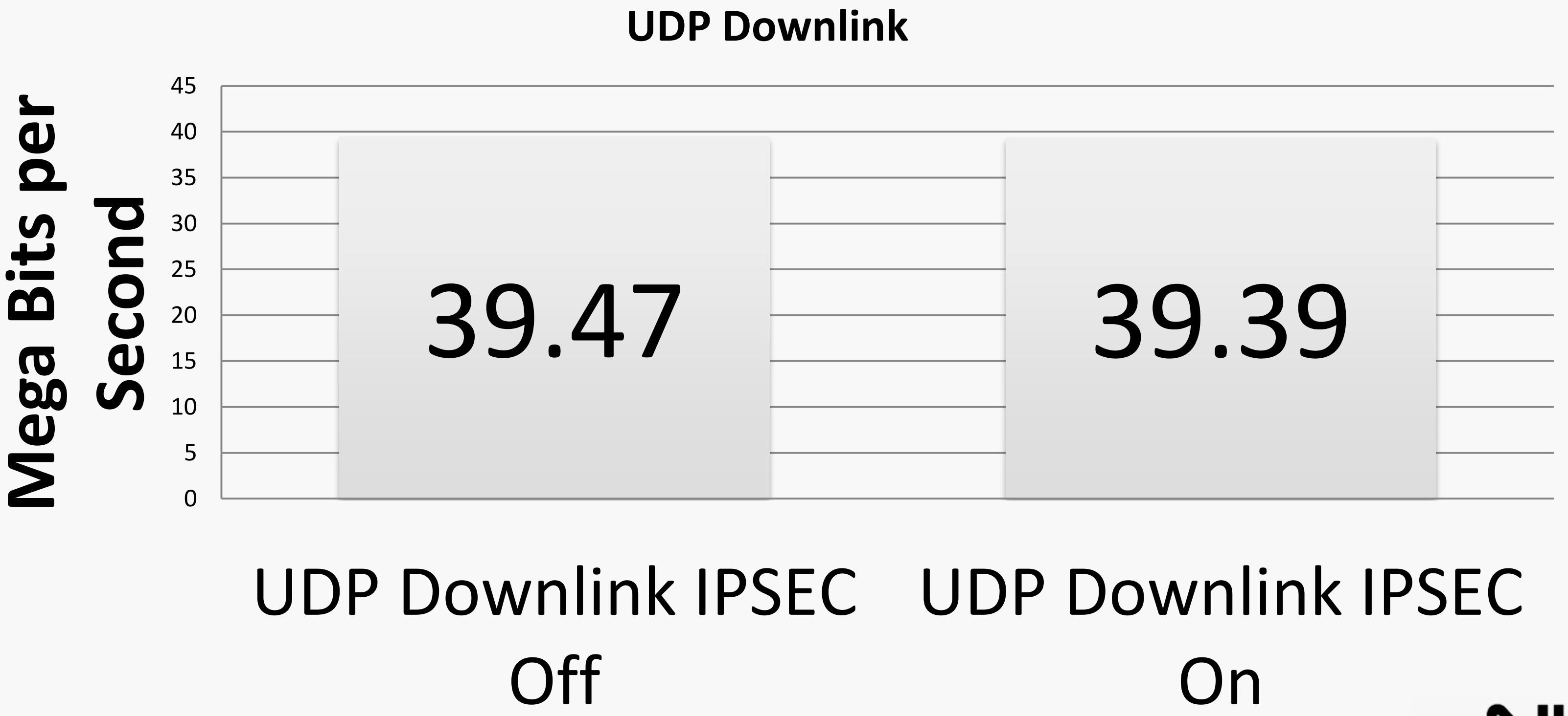
Encrypted Traffic

No.	Time	Source	Destination	Protocol	Length	Info
1200	14.274868000	10.8.98.98	10.8.98.2	ESP	198	ESP (SPI=0x81d74104)
1201	14.275698000	10.8.98.98	10.8.98.2	ESP	198	ESP (SPI=0x81d74104)
1202	14.276185000	10.8.98.2	10.8.98.98	ESP	150	ESP (SPI=0xc985ae27)
1203	14.285995000	10.8.98.98	10.8.98.2	ESP	358	ESP (SPI=0x81d74104)
1204	14.286013000	10.8.98.98	10.8.98.2	ESP	150	ESP (SPI=0x81d74104)
1205	14.286015000	10.8.98.98	10.8.98.2	ESP	198	ESP (SPI=0x81d74104)
1206	14.286017000	10.8.98.98	10.8.98.2	ESP	150	ESP (SPI=0x81d74104)
1207	14.286019000	10.8.98.98	10.8.98.2	ESP	150	ESP (SPI=0x81d74104)
1208	14.286926000	10.8.98.2	10.8.98.98	ESP	438	ESP (SPI=0xc985ae27)
1209	14.286941000	10.8.98.98	10.8.98.2	ESP	278	ESP (SPI=0x81d74104)
1210	14.286943000	10.8.98.2	10.8.98.98	ESP	1510	ESP (SPI=0xc985ae27)
1211	14.287040000	10.8.98.2	10.8.98.98	ESP	118	ESP (SPI=0xc985ae27)
1212	14.287045000	10.8.98.2	10.8.98.98	ESP	182	ESP (SPI=0xc985ae27)
1213	14.287046000	10.8.98.2	10.8.98.98	ESP	1510	ESP (SPI=0xc985ae27)
1214	14.287049000	10.8.98.2	10.8.98.98	ESP	118	ESP (SPI=0xc985ae27)
1215	14.287051000	10.8.98.2	10.8.98.98	ESP	198	ESP (SPI=0xc985ae27)
1216	14.287052000	10.8.98.2	10.8.98.98	ESP	1190	ESP (SPI=0xc985ae27)
1217	14.292855000	10.8.98.98	10.8.98.2	ESP	214	ESP (SPI=0x81d74104)
1218	14.301919000	10.8.98.98	10.8.98.2	ESP	198	ESP (SPI=0x81d74104)
1219	14.303757000	10.8.98.98	10.8.98.2	ESP	198	ESP (SPI=0x81d74104)
1220	14.306218000	10.8.98.98	10.8.98.2	ESP	390	ESP (SPI=0x81d74104)
1221	14.306250000	10.8.98.98	10.8.98.2	ESP	150	ESP (SPI=0x81d74104)
1222	14.306805000	10.8.98.2	10.8.98.98	ESP	1510	ESP (SPI=0xc985ae27)
1223	14.306823000	10.8.98.2	10.8.98.98	ESP	118	ESP (SPI=0xc985ae27)
1224	14.308001000	10.8.98.2	10.8.98.98	ESP	230	ESP (SPI=0xc985ae27)
1225	14.308014000	10.8.98.2	10.8.98.98	ESP	1510	ESP (SPI=0xc985ae27)
1226	14.308027000	10.8.98.2	10.8.98.98	ESP	118	ESP (SPI=0xc985ae27)
1227	14.308029000	10.8.98.2	10.8.98.98	ESP	182	ESP (SPI=0xc985ae27)
1228	14.308030000	10.8.98.2	10.8.98.98	ESP	1510	ESP (SPI=0xc985ae27)
1229	14.308033000	10.8.98.2	10.8.98.98	ESP	118	ESP (SPI=0xc985ae27)
1230	14.308034000	10.8.98.2	10.8.98.98	ESP	182	ESP (SPI=0xc985ae27)

```
▷ Frame 1225: 1510 bytes on wire (12080 bits), 1510 bytes captured (12080 bits) on interface 0
▷ Ethernet II, Src: 44:f4:77:8e:0b:98 (44:f4:77:8e:0b:98), Dst: 58:8d:09:be:d7:40 (58:8d:09:be:d7:40)
▷ Internet Protocol Version 4, Src: 10.8.98.2 (10.8.98.2), Dst: 10.8.98.98 (10.8.98.98)
▽ Encapsulating Security Payload
    ESP SPI: 0xc985ae27 (3380981287)
    ESP Sequence: 613
```

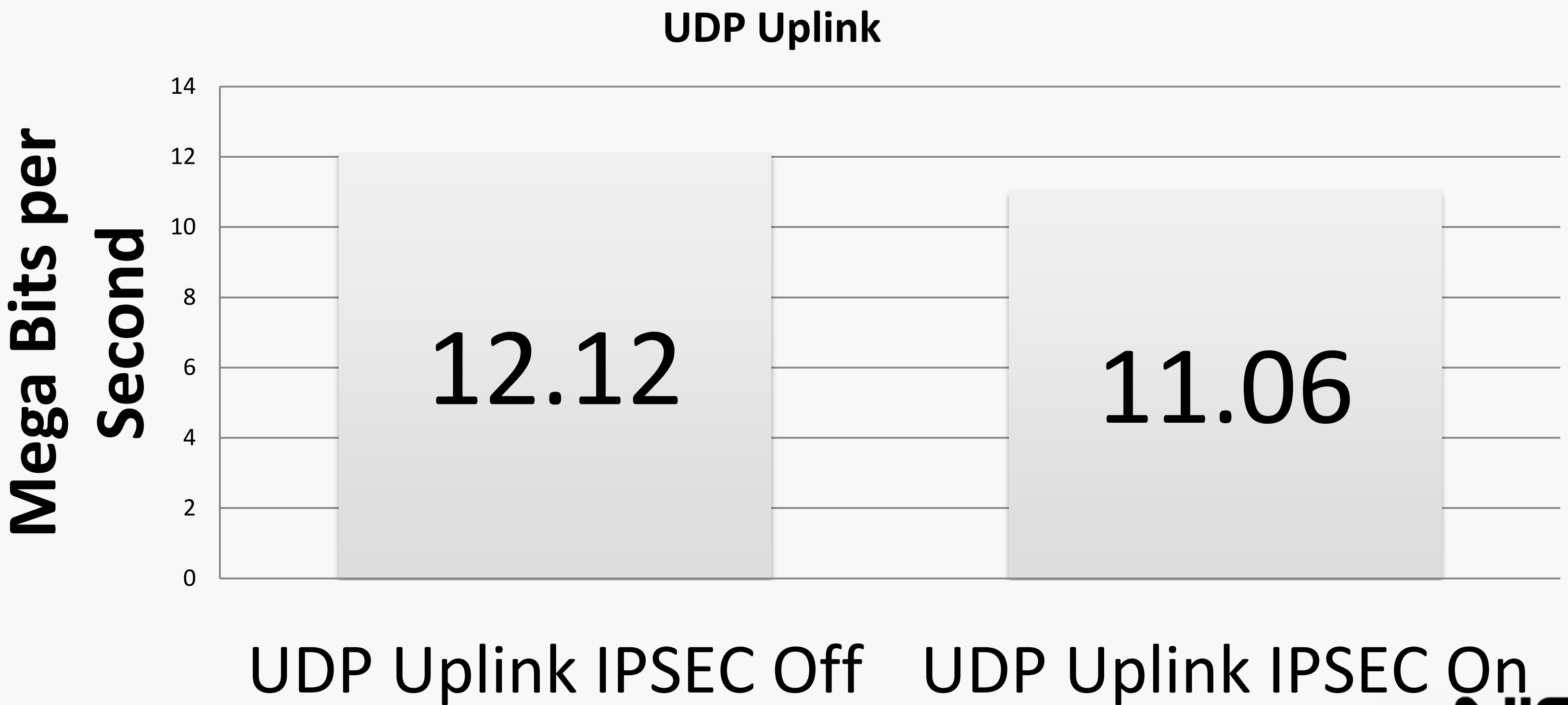
National Institute of Standards and Technology
U.S. Department of Commerce

Initial Performance Results



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

Initial Performance Results



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

Next Steps

- Identify additional more tests to better simulate real world deployments.
  - Simulate multiple base stations connecting to one security gateway
  - Interoperability tests
- Identify other vulnerable network interfaces to secure.
  - Uu

Threats to LTE Networks

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

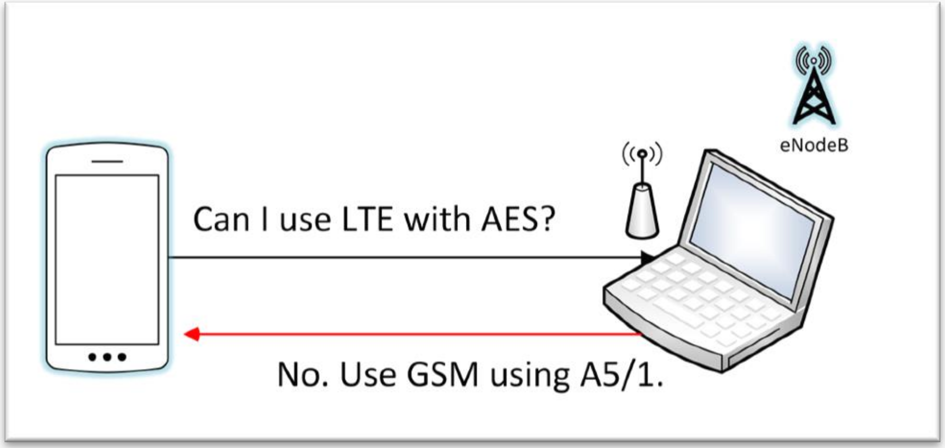
General Computer Security Threats

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

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

Renegotiation Attacks

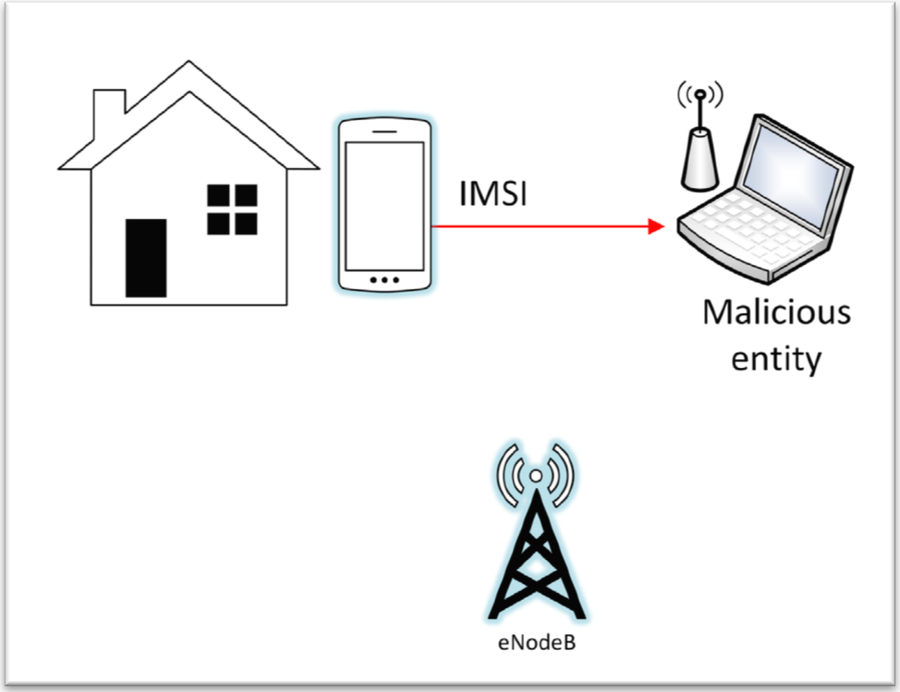
- **Threat:** Rogue base stations can force a user to downgrade to GSM or UMTS.
  - Significant weaknesses exist in GSM cryptographic algorithms.
- **Mitigation:**
  - Ensure LTE network connection. Most current mobile devices do not provide the ability to ensure a user's mobile device is connected to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



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

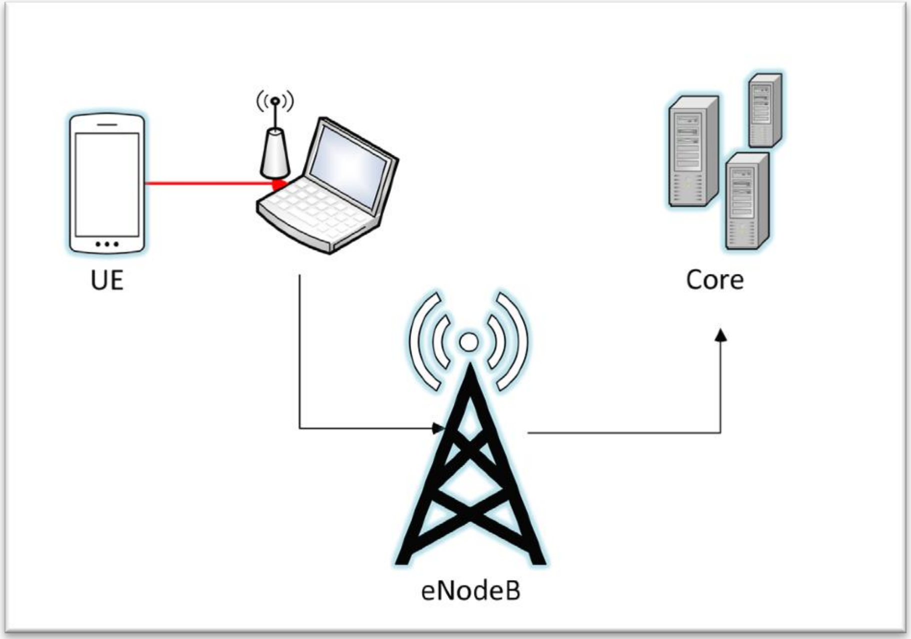
Device & Identity Tracking

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



Call Interception

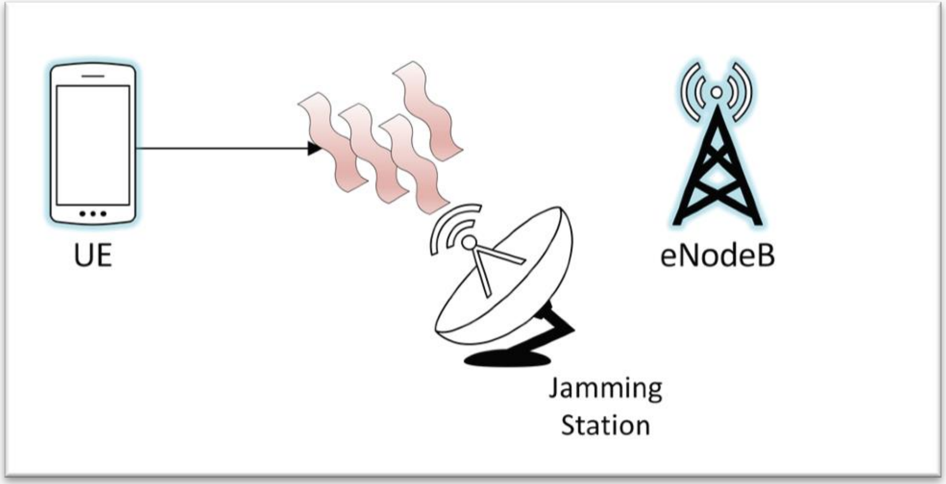
- **Threat:** Renegotiation attacks may also allow MitM attacks to establish an unencrypted connection to a device making a phone call
  - Attacker may be able to listen to the phone call
- **Mitigation:** The ciphering indicator feature discussed in 3GPP TS 22.101 would alert the user if calls are made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



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

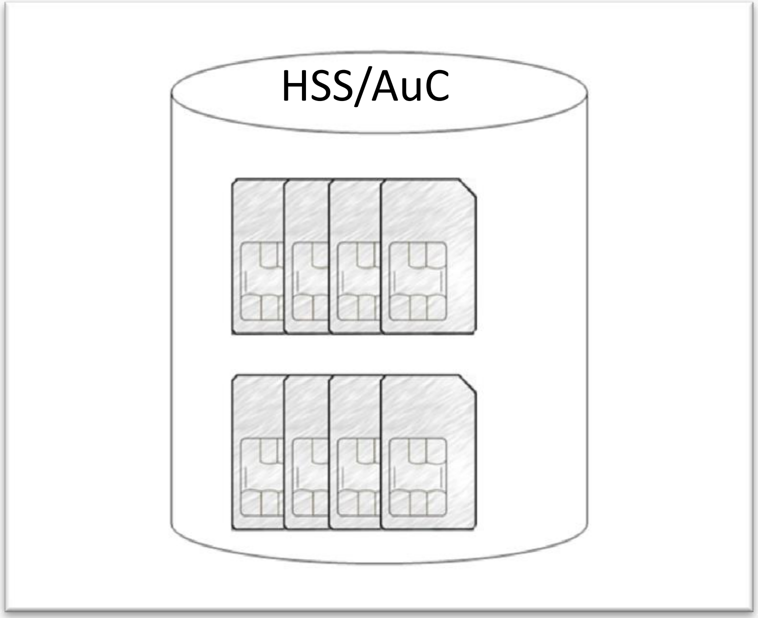
Jamming UE Radio Interface

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



Attacks Against the Secret Key (K)

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



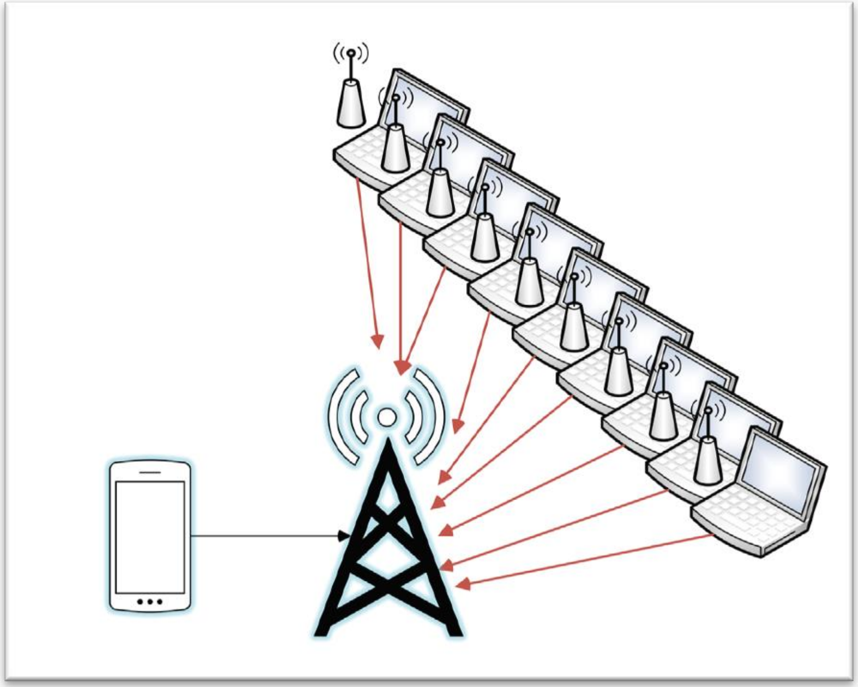
Physical Base Station Attacks

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

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

Availability Attacks on eNodeB & Core

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



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?

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

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
eNodeB	Evolved 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.