Cellular Radio “Null Ciphers” & Android

Yomna Nasser

Android Connectivity Security Team

yomna@google.com

Talk overview

- How do cellular networks (fail) to use cryptography to ensure confidentiality and integrity?
- What is Android doing about it?
- What kinds of challenges come up when making radio security improvements?

Terminology

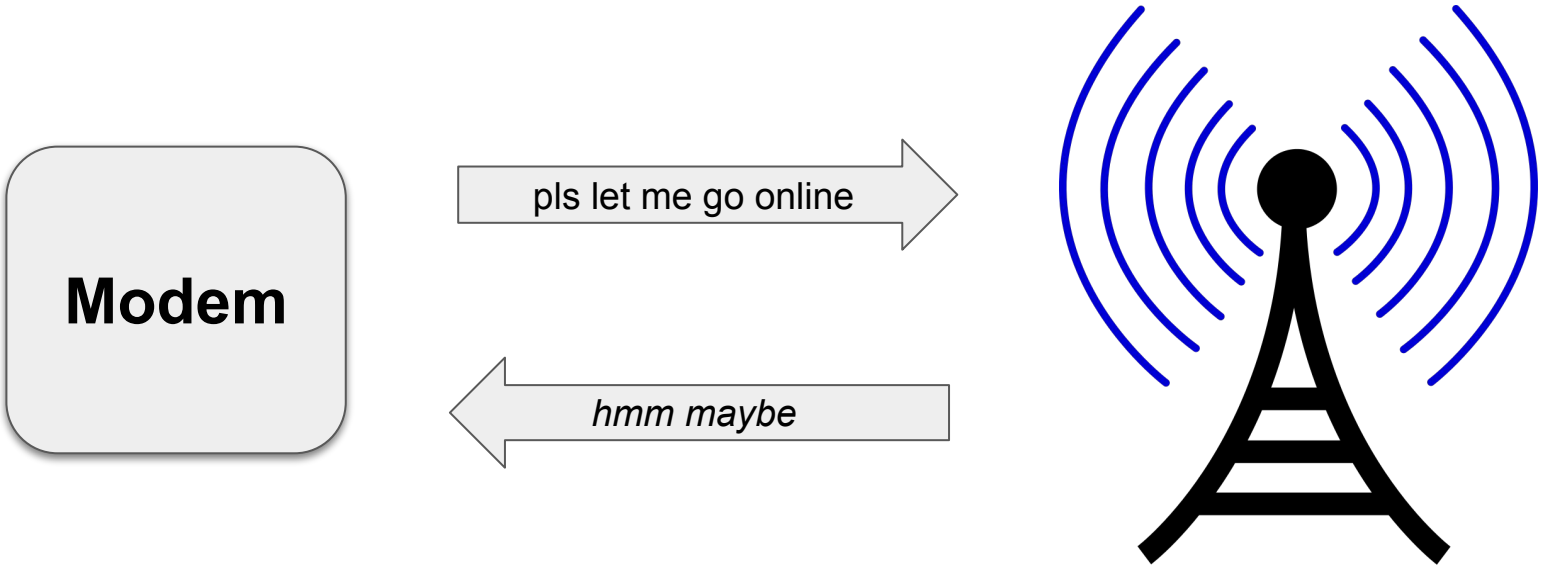
- **Cell “towers” ***
  - Base station (BTS)
  - Cell site
  - eNodeB (in LTE)

- **Network generations**
  - 2G (GSM)
  - 3G
  - 4G (LTE)
  - 5G

- **Fake base station (FBS)**
  - Cell Site Simulator
  - IMSI-catcher
  - Stingray (brandname)
  - Rogue cell tower
  - Rogue base station
  - “Attacker”

* Everything in cellular has many names. Also, in urban areas instead of cell “towers” it’s often just antennas mounted on buildings.

Cellular connections

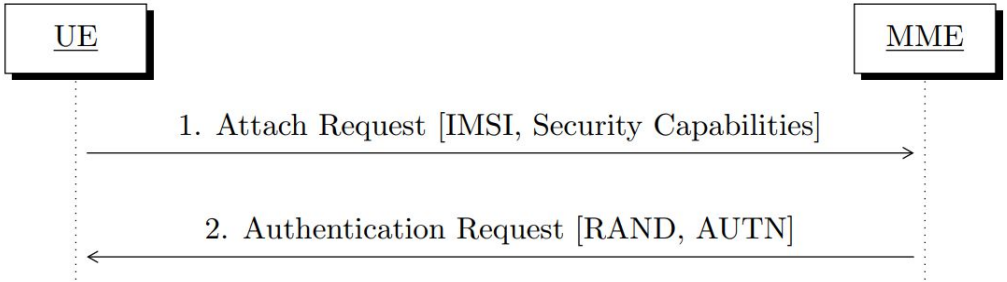


* The “modem” is often also called: radio / baseband / CP (Communications Processor).

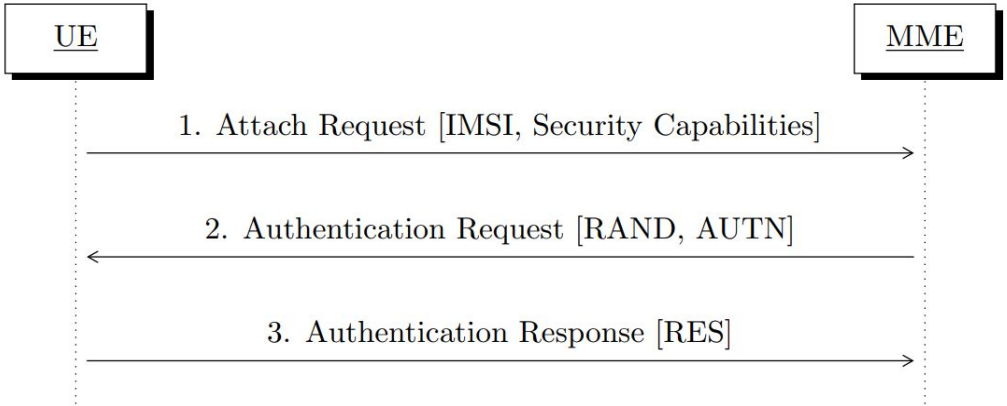
** “User equipment” or “UE” = general term for user’s phone + modem.

Initial Attach Procedure (LTE)

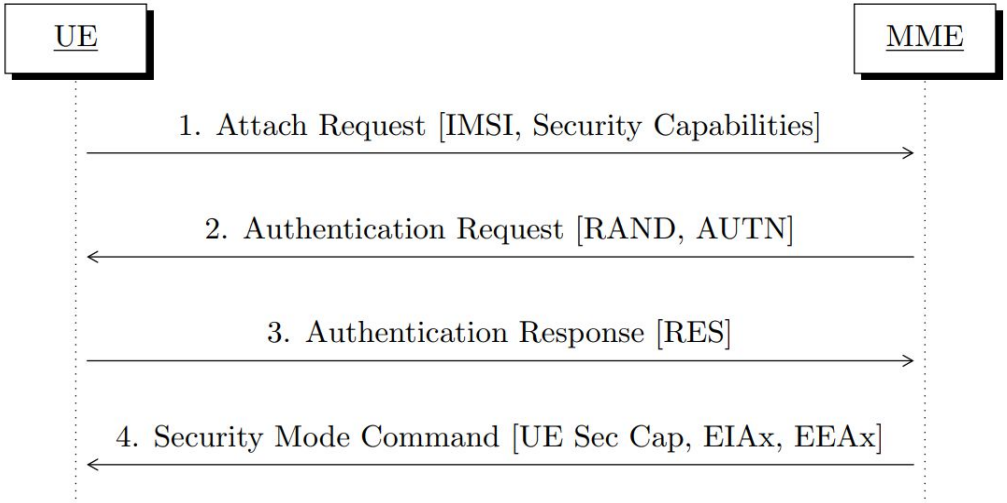
Initial Attach Procedure (LTE)



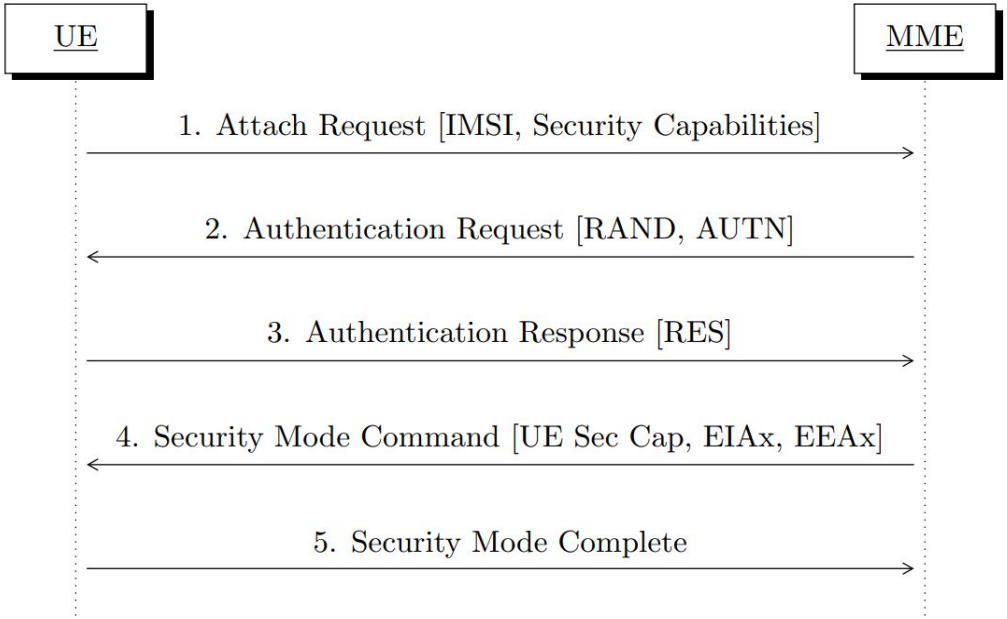
Initial Attach Procedure (LTE)



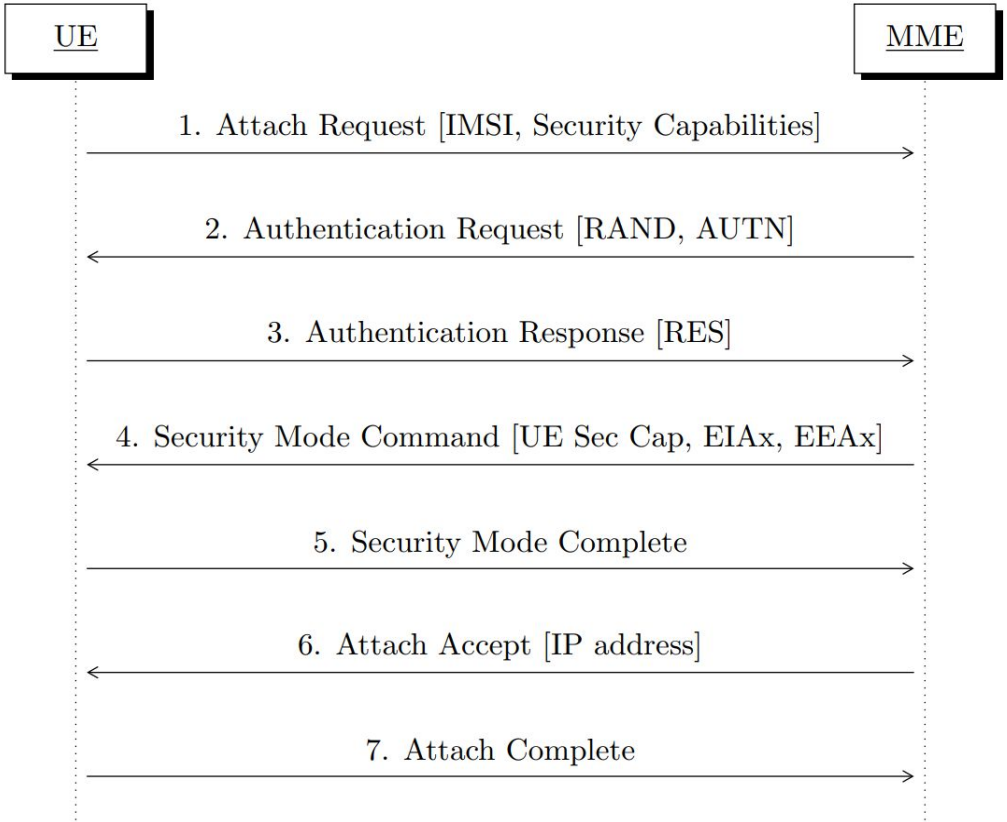
Initial Attach Procedure (LTE)



Initial Attach Procedure (LTE)



Initial Attach Procedure (LTE)



3GPP/GSMA Cryptographic Algorithms

Algorithms for authentication and key generation:

Cipher	Proprietary	Proprietary	Proprietary	AES	Keccak
Input key size	128	128	128	128	128, 256
Output key size	54	54	64	128	128, 256
Name	COMP-128-1	COMP-128-2	COMP-128-3	MILENAGE	Tuak

Algorithms for encryption and integrity:

Cipher	Proprietary	Proprietary	KASUMI	KASUMI	KASUMI	SNOW 3G	SNOW 3G	AES	AES	ZUC	ZUC
Key size	64	64	64	128	128	128	128	128	128	128	128
Mode	XOR	XOR	f8-mode	f8-mode	CBC-MAC	XOR	CW-MAC1	CTR	CMAC	XOR	CW-MAC2
Type	ENC	ENC	ENC	ENC	INT	ENC	INT	ENC	INT	ENC	INT
2G GSM	A5/1	A5/2	A5/3	A5/4							
2G GPRS	GEA1	GIA2	GEA3	GEA4	GIA4	GEA5	GIA5				
3G UMTS				UEA1	UIA1	UEA2	UIA2				
4G LTE						128-EEA1	128-EIA1	128-EEA2	128-EIA2	128-EEA3	128-EIA3
5G NR						128-NEA1	128-NIA1	128-NEA2	128-NIA2	128-NEA3	128-NIA3

Null versions:

- 2G GSM:
  - A5/0 (encryption)
  - No integrity in GSM
- 2G GPRS:
  - GEA0 (encryption)
  - GIA0 (integrity)
- 3G UMTS:
  - UEA0
  - UIA0
- 4G LTE:
  - EEA0
  - EIA0
- 5G:
  - NEA0
  - NIA0

Image from IETF / John Mattson (Ericsson): https://datatracker.ietf.org/meeting/104/materials/slides-104-saag-snow-v-stream-cipher-00

Paper 2021/819

Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2

Christof Beierle, Patrick Derbez, Gregor Leander, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, and Lukas Stennes

Abstract

This paper presents the first publicly available cryptanalytic attacks on the GEA-1 and GEA-2 algorithms. Instead of providing full 64-bit security, we show that the initial state of GEA-1 can be recovered from as little as 65 bits of known keystream (with at least 24 bits coming from one frame) in time 2^{40} GEA-1 evaluations and using

A sad reality

- Lots of carriers just don't use encryption or integrity protection

	GEA0	GEA1	GEA2	GEA3	Total unique operators
Americas	4	0	1	3	8
Europe	10	0	2	43	55
Africa	19	0	1	6	26
Asia	5	0	0	6	11

Table–1: Number of operators assigning a specific cipher per region, main algorithm only (collected in 2019, 2020, 2021)

- Difficult for security researchers to help out

Table 1 from Umlaut: https://www.umlaut.com/uploads/documents/20210615_Analysis_of_EGPRS_ciphering_algorithms.pdf

LTE Security Disabled—Misconfiguration in Commercial Networks

Merlin Chlosta
merlin.chlosta@rub.de
Ruhr University Bochum
Germany

David Rupprecht
david.rupprecht@rub.de
Ruhr University Bochum
Germany

Thorsten Holz
thorsten.holz@rub.de
Ruhr University Bochum
Germany

Christina Pöpper
christina.poepper@nyu.edu
NYU Abu Dhabi
United Arab Emirates

ABSTRACT

Long Term Evolution (LTE) is the de-facto standard for mobile communication. It provides effective security features but leaves room for misunderstandings in its configuration and implementation. In

The security goals of LTE aim to provide mutual authentication, integrity and confidentiality of traffic, and location privacy. These goals and their consideration in the specification evolved from the lessons learned of previous cellular generations. Flaws and

Primary (legit) use cases for null ciphering/integrity

🕵️ Debugging by carriers/network operators

🚒 Emergency calls when you don’t have an active SIM card

🏺 Fallback in case networks deprecate all other encryption algorithms the modem is programmed to use [1]

[1] *GSMA Security Algorithm Roadmap*

Cellular security matters

- Fundamental cellular infrastructure should be as secure as possible, even if we view parts of it as outdated.

- Classic voice calls and SMS aren’t going away any time soon for most people.

- Cellular radio attacks are becoming more common, easier to pull off.

Paris IMSI-Catcher Mistaken for Bomb Was Actually Used for Health Insurance SMS Phishing Scam

Article from Commsrisk, published Feb 21 2023

Newly supported in Android 14

✨ You can choose to only use encrypted connections now ✨

- Encryption requirement applies to all parts of cellular radio connection which support encryption.
- Integrity-protection is now required on all SMS & voice call traffic.
  - Modems generally are not able to support integrity-protection for mobile data due to historical & performance issues.

Newly supported in Android 14

✨ You can choose to only use encrypted connections now ✨

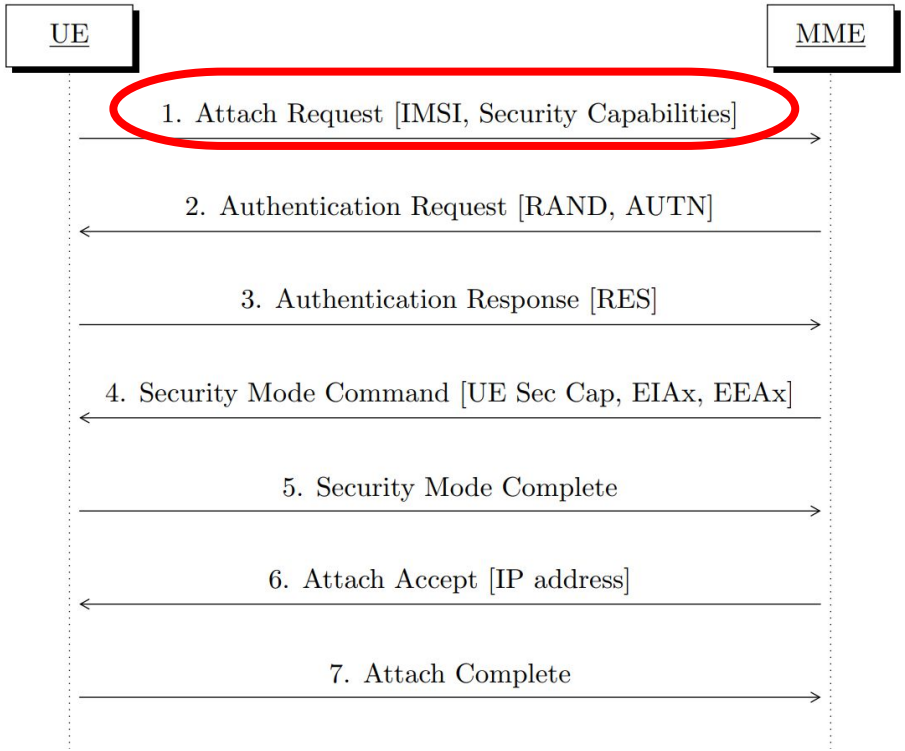
- Encryption requirement applies to all parts of cellular radio connection which support encryption.
- Integrity-protection is now required on all SMS & voice call traffic.
  - Modems generally are not able to support integrity-protection for mobile data due to historical & performance issues.
- **Note: this is not related to core network encryption!**

Newly supported in Android 14

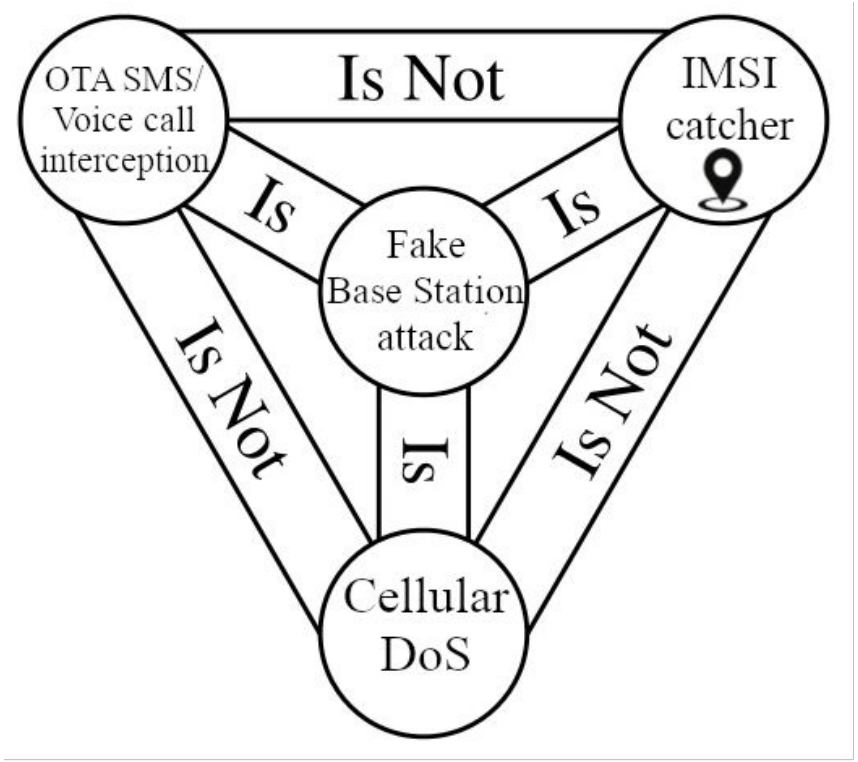
✨ You can choose to only use encrypted connections now ✨

- Encryption requirement applies to all parts of cellular radio connection which support encryption.
- Integrity-protection is now required on all SMS & voice call traffic.
  - Modems generally are not able to support integrity-protection for mobile data due to historical & performance issues.
- Note: this is not related to core network encryption!
- **Note: probably requires hardware upgrades.**

Caveat: “IMSI-catcher” / FBS mean **many** different things



Step 1 is the key part of the classic “IMSI-catching” attack!



Implementation details: Android <> modem API

We are here —>

This is where we specify APIs between Android and hardware components.

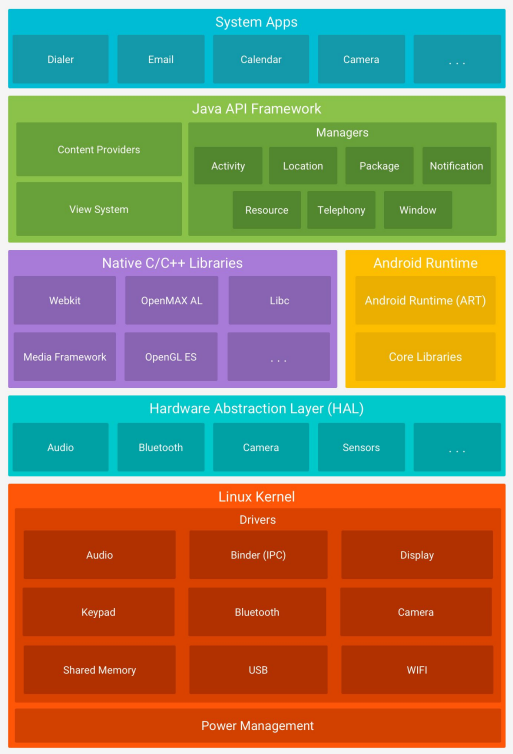
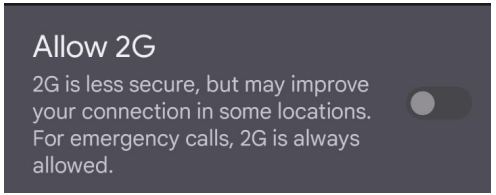


Diagram of Android OS internal layout

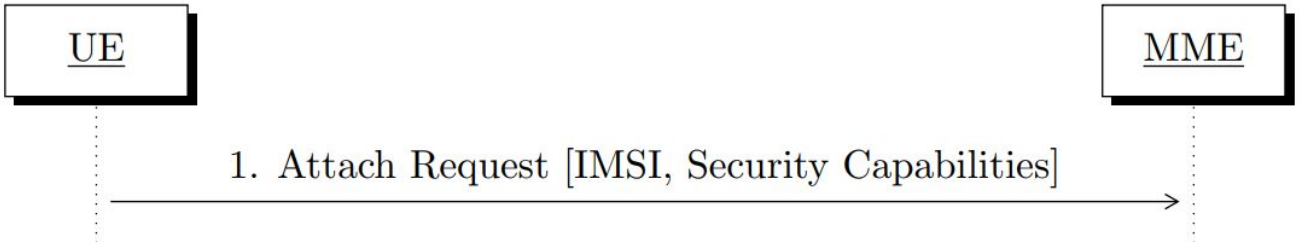
Past example API

```
/**
 * Requests to set the network type for searching and registering.
 *
 * Instruct the radio to *only* accept the types of network provided.
 * setPreferredNetworkType, setPreferredNetworkTypesBitmap will not be called anymore
 * except for IRadio v1.5 or older devices.
 *
 * In case of an emergency call, the modem is authorized to bypass this
 * restriction.
 *
 * @param serial Serial number of request.
 * @param networkTypeBitmap a 32-bit bearer bitmap of RadioAccessFamily
 *
 * Response callback is IRadioResponse.setAllowedNetworkTypesBitmapResponse()
 */
oneway setAllowedNetworkTypesBitmap(
        uint32_t serial, bitfield<RadioAccessFamily> networkTypeBitmap);
```



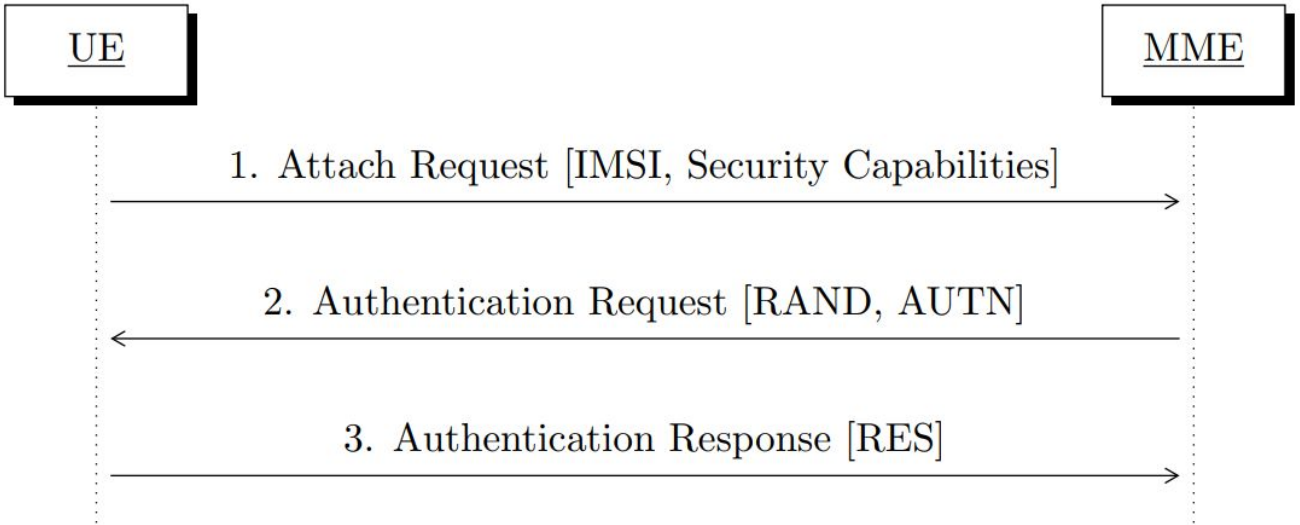
From: https://cs.android.com/android/platform/superproject/+/master:hardware/interfaces/radio/1.6/IRadio.hal

Implementation details: new connection flow? (Example 1)

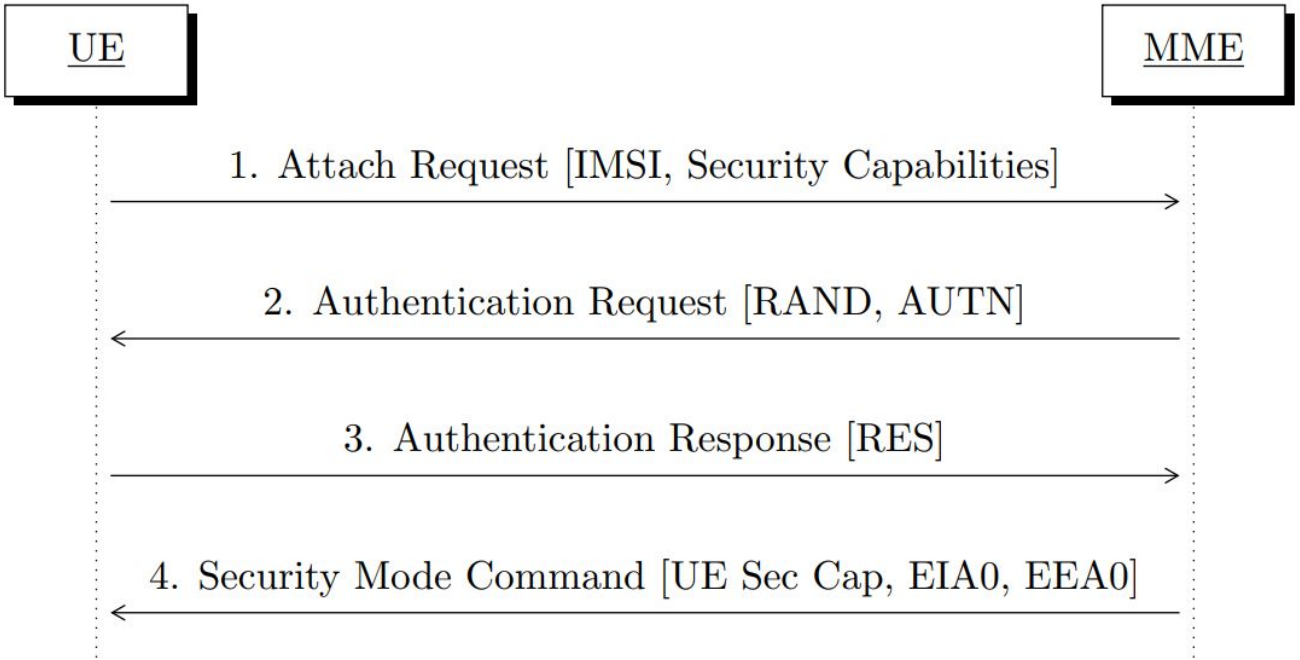


Implementation details: new connection flow? (Example 1)

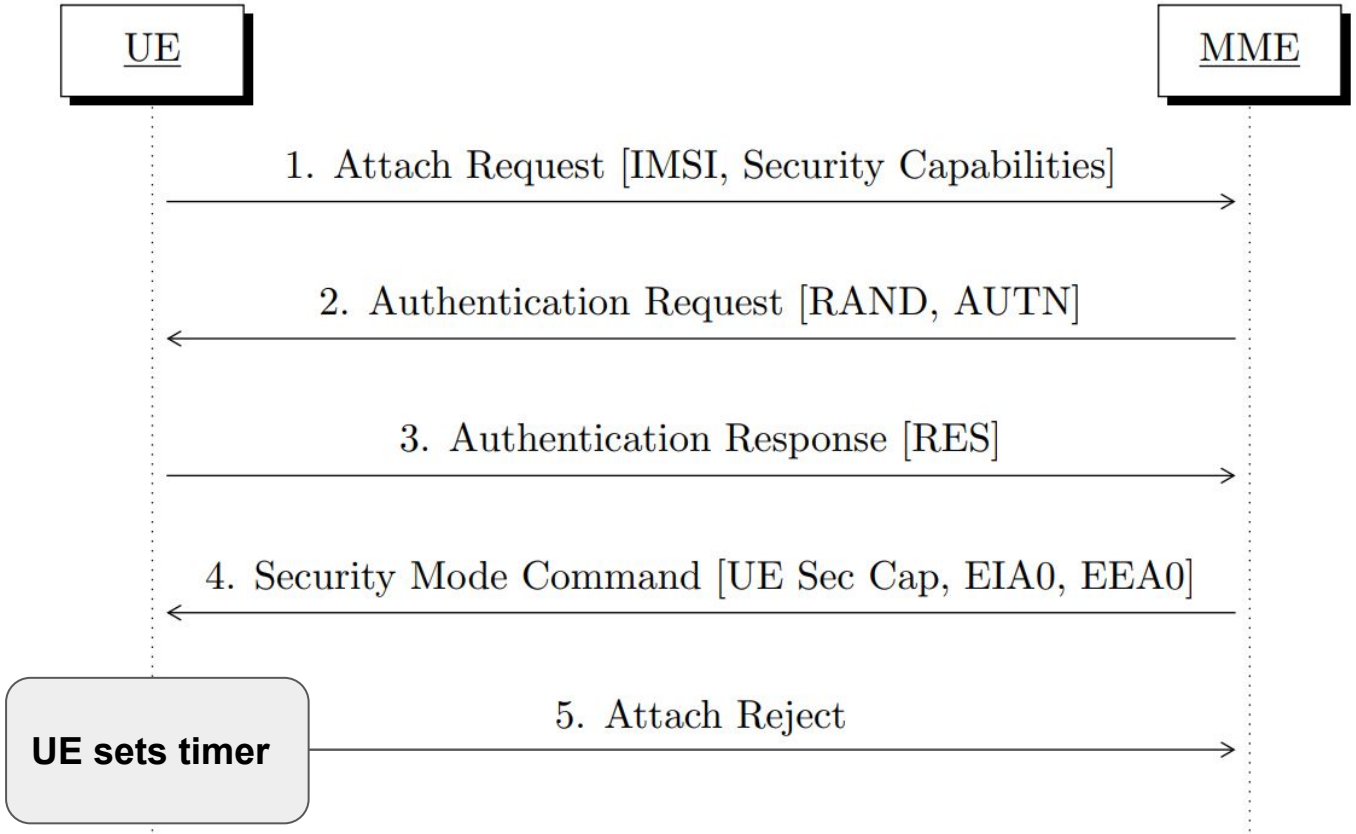
Implementation details: new connection flow? (Example 1)



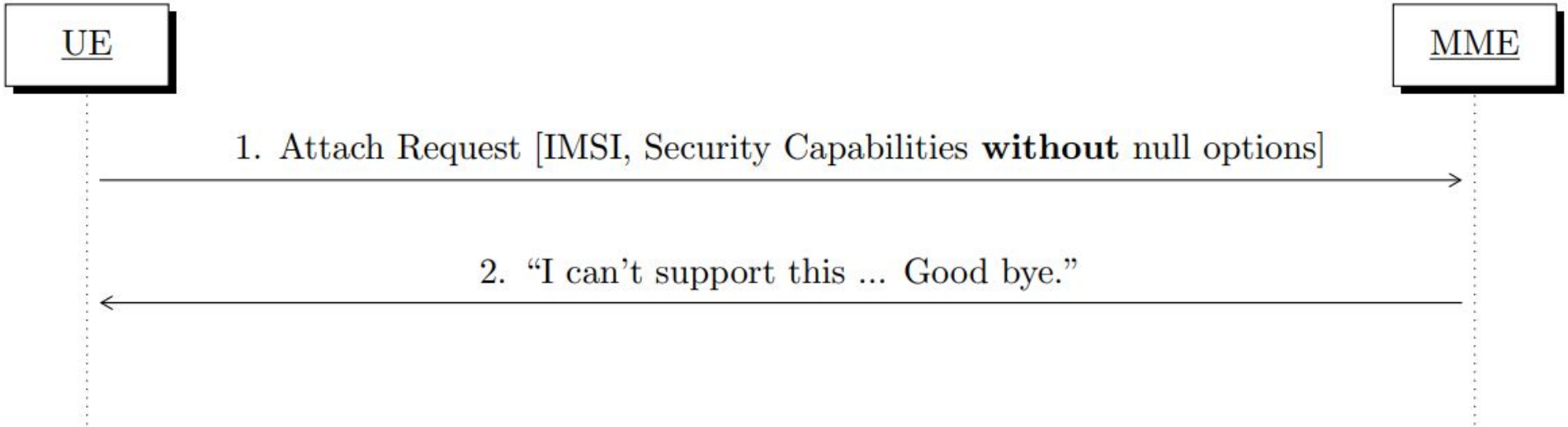
Implementation details: new connection flow? (Example 1)



Implementation details: new connection flow? (Example 1)



Implementation details: new connection flow? (Example 2)



Further reading

- ***Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks*** (2019): https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks

- ***LTE security disabled: misconfiguration in commercial networks*** by Merlin Chlosta, David Rupprecht, Thorsten Holz, Christina Pöpper: https://dl.acm.org/doi/10.1145/3317549.3324927

Thanks to: Roger Piqueras Jover, Gil Cukierman, and Dominik Maier :)