Tutorial: *“5G and O-RAN Security Review Towards 6G: Security and Privacy Attacks on Cellular Networks”*

First Summer School on Security and Privacy in 6G Networks

Universidad Complutense de Madrid

Madrid, June 24-28

Team: **Esteban Municio, Ginés García, Oscar Lasierra, Pau Baguer, Xavier Costa**

i2cat

Never stop designing the digital future

i2CAT.net

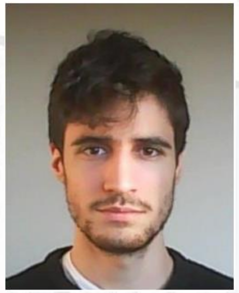
CERCA Centres de Recerca de Catalunya

tecnio catalonia ACCIÓ Generalitat de Catalunya

Tutorial Team

Esteban Municio

Ginés García



Óscar Lasierra

Pau Baguer

Xavier Costa

5G and O-RAN Security Review Towards 6G

Security and Privacy attacks on Cellular Networks

Part 1: From 4G to 5G Systems Security

Theory

Esteban Municio

Ginés García

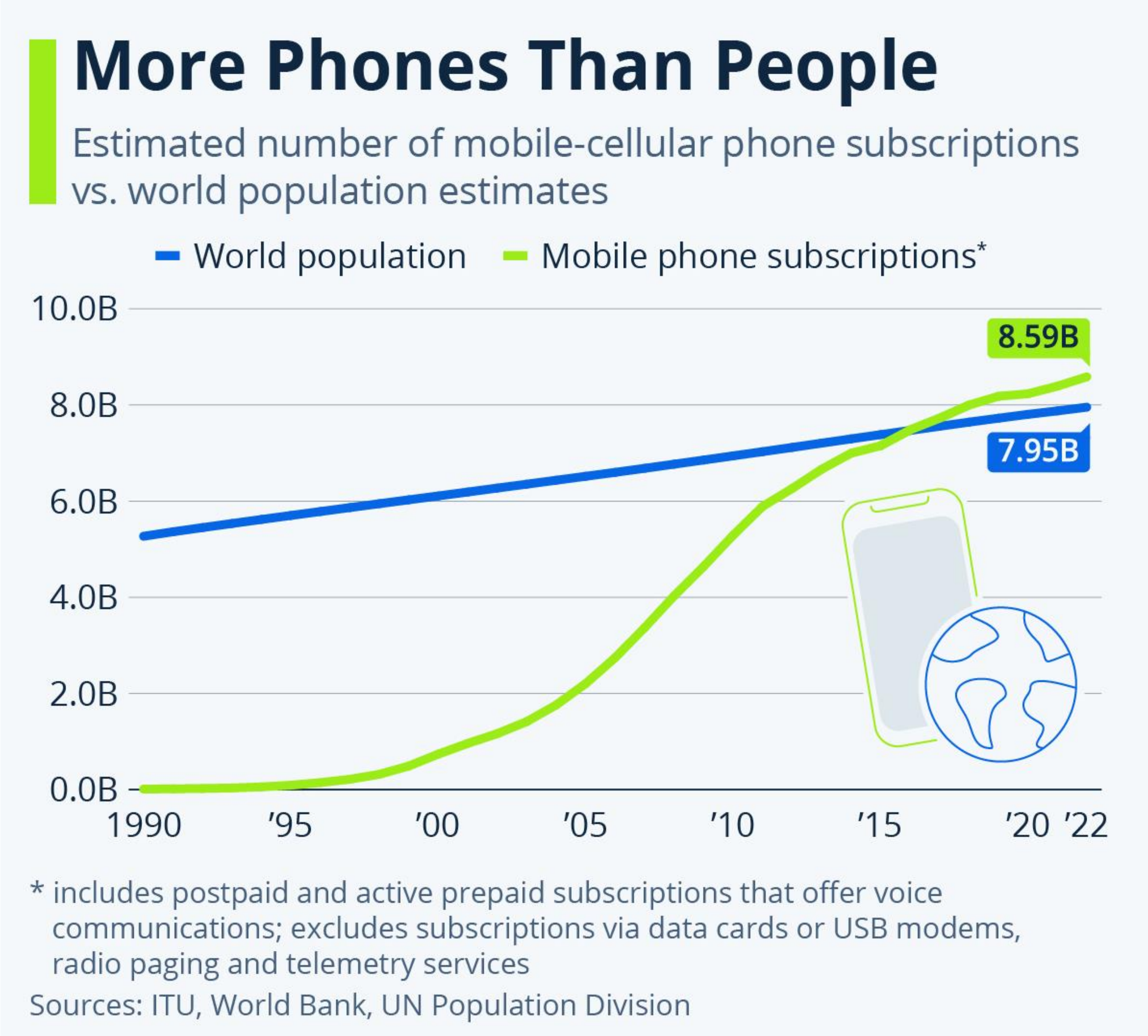
Xavier Costa

i2cat

Mobile Networks Security

Why do we care?

Mobile Networks Security – Why do we care?



Mobile Networks Security – Why do we care?

ALJAZEERA News Israel War on Gaza Features Opinion Sport Video

News | Telecommunications

US firm AT&T says data of 73 million customers leaked on ‘dark web’

At least 7.6 million existing AT&T account holders and 65.4 million former users hit by the breach, the company says.

March 24

FORBES › BUSINESS

BREAKING

T-Mobile Data Breach: Hackers Stole 37 Million Customers’ Info, Company Says

Nicholas Reimann Forbes Staff
News and explainers.

Follow

Jan 19, 2023, 06:32pm EST

Updated Jan 20, 2023, 10:57am EST

TOPLINE Around 37 million T-Mobile customers recently had their personal information compromised in the company’s second major hack in less than two years, the company said Thursday, adding hackers were able to access customers’ names, addresses and dates of birth but not highly sensitive financial information like Social Security and credit card numbers.

FORBES › MONEY › PERSONAL FINANCE

T-Mobile’s Hack Of 50 Million Users Leaves Black Community At Risk

Kori Hale Contributor
I’m the CEO of CultureBanx, redefining business news for minorities.

Follow

Sep 10, 2021, 08:00am EDT

Updated Sep 13, 2021, 07:50am EDT

This article is more than 2 years old.

People pass a T-Mobile store, in New York, Wednesday, Oct. 14, 2015. The top Democrat on the Senate ... [+] ASSOCIATED PRESS

T-Mobile claims it has notified nearly all of the 50 million customers whose personal data was stolen in the company’s largest ever data breach. Currently it has 38% of the U.S. prepaid market, and if you look

5G Security

New Features Review

Why is 5G more Secure?

4G Vulnerabilities	5G SA
No concealment of permanent identifiers. No specific policies for GUTI reallocation.	Concealment of SUPI, the SUCI. GUTI reallocation after Registration and Service Request.
Lack of randomness and the use of XOR in AUTS	New 5G-AKA supported by the new Core NFs
UP Confidentiality Optional Support	UP Confidentiality Mandatory Support
UP Integrity Optional Support	UP Integrity Mandatory Support
No security for initial NAS message	Mandatory protection of Initial NAS message

5G Security Enhancements

Subscriber Identifiers

5G Primary Authentication

CP and UP Security

UE Security Capabilities

SUPI: Subscription Permanent Identifier

SUCI: Subscription Concealed Identifier

<u>Enhancements</u>:

Concealment of permanent identifiers

5G Security Enhancements

Subscriber Identifiers

5G Primary Authentication

CP and UP Security

UE Security Capabilities

SUPI: Subscription Permanent Identifier

SUCI: Subscription Concealed Identifier

5G-GUTI: 5G Global Unique Temporary Identifier

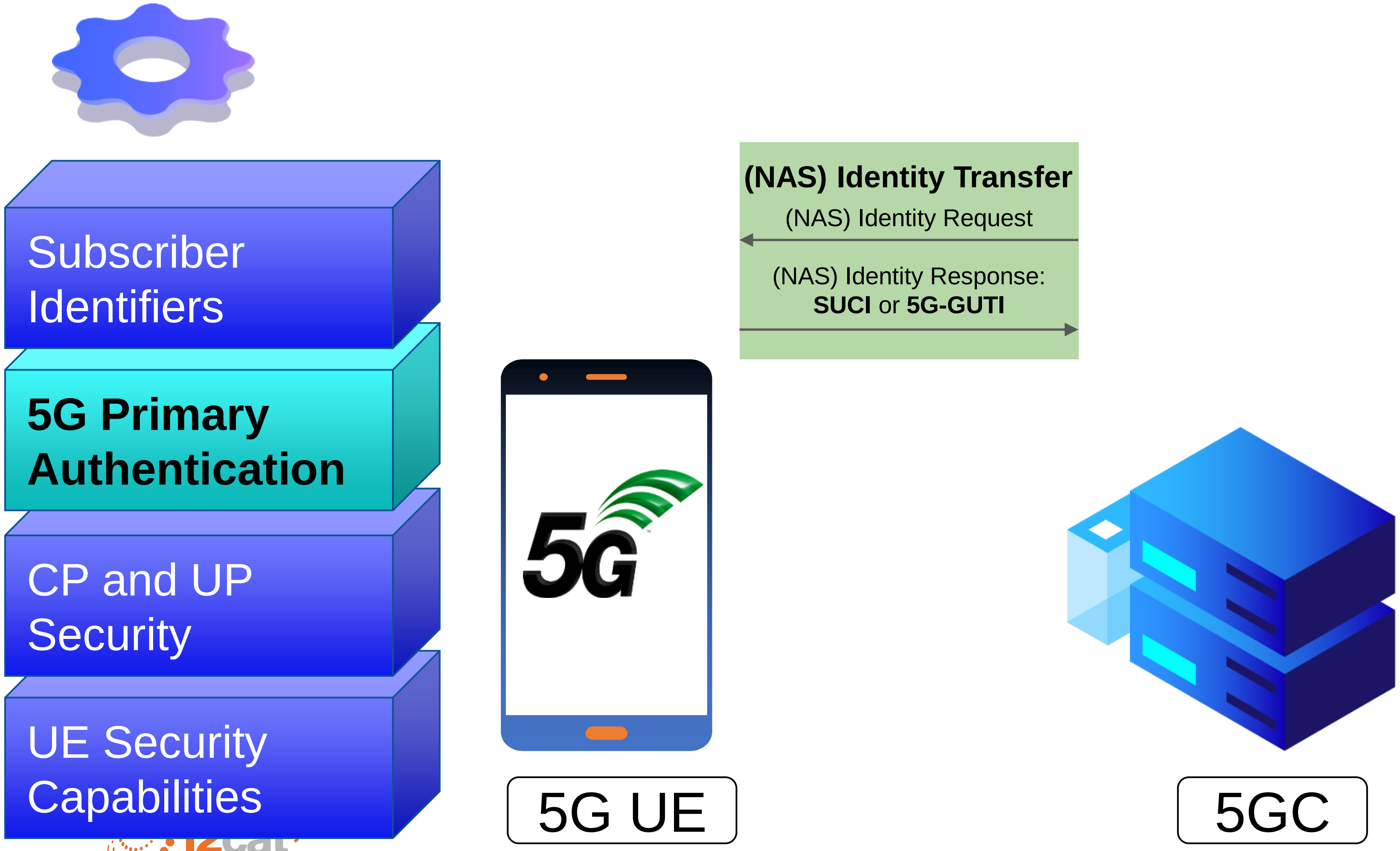
5G-TMSI: 5G Temporary Mobile Subscriber Identity

Enhancements:

Concealment of permanent identifiers

New 5G-GUTI value upon receiving **Registration Request** and **Service Request** messages

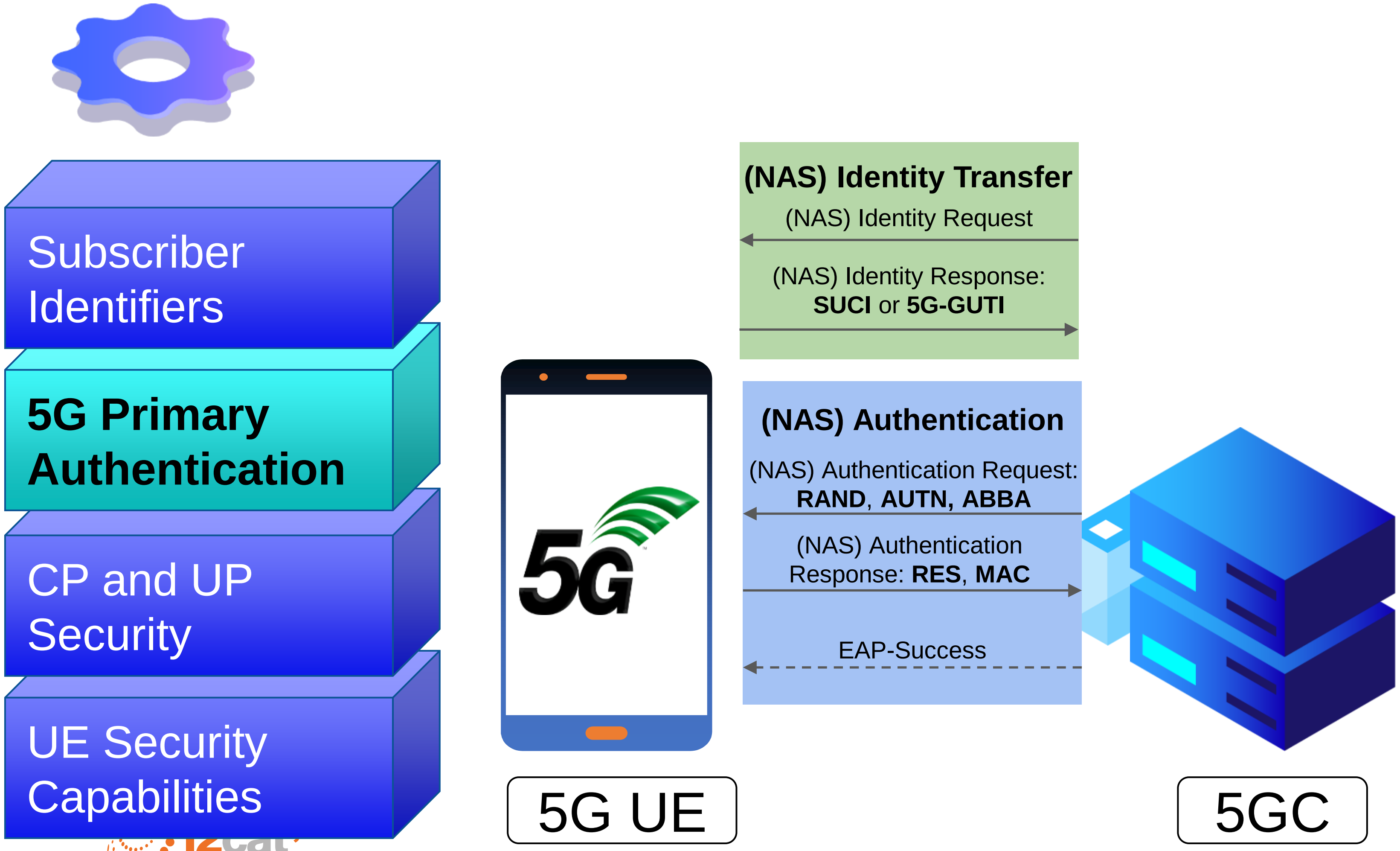
5G Security Enhancements



Enhancements:

Three new authentication methods: **5G-AKA, EAP-AKA’** and **EAP-TLS**

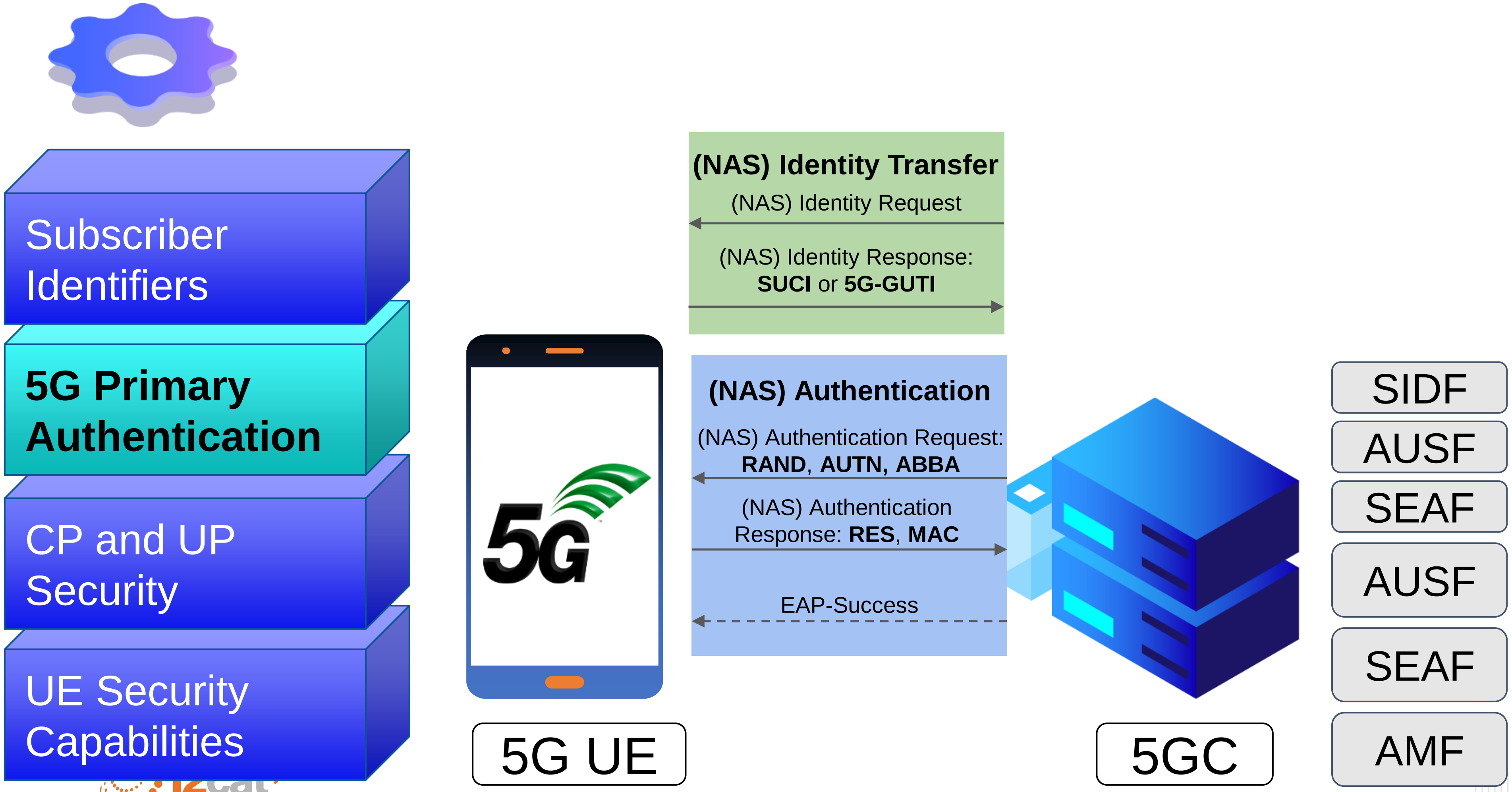
5G Security Enhancements



Enhancements:

Three new authentication methods: **5G-AKA, EAP-AKA'** and **EAP-TLS**

5G Security Enhancements

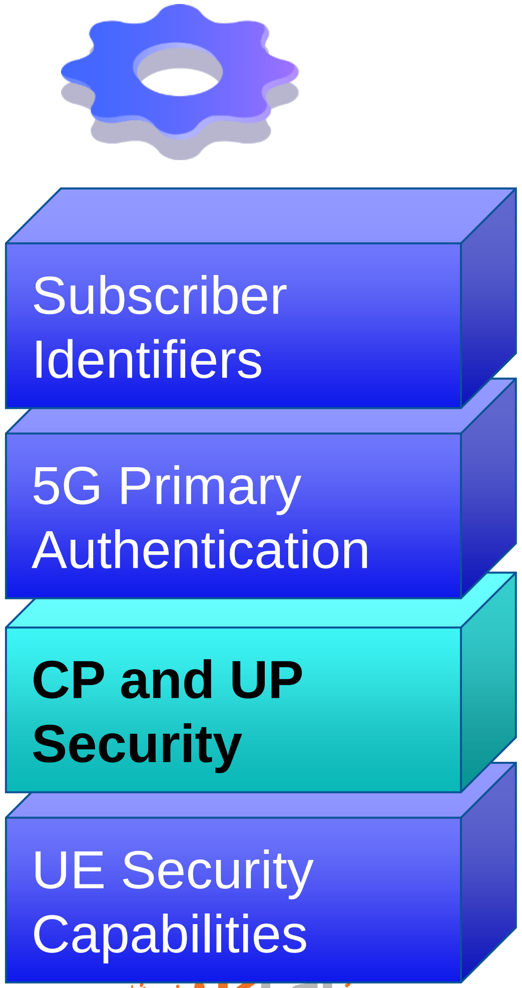


Enhancements:

Three new authentication methods: **5G-AKA, EAP-AKA’** and **EAP-TLS**

Service based architecture, Network Functions are taking active roles

5G Security Enhancements

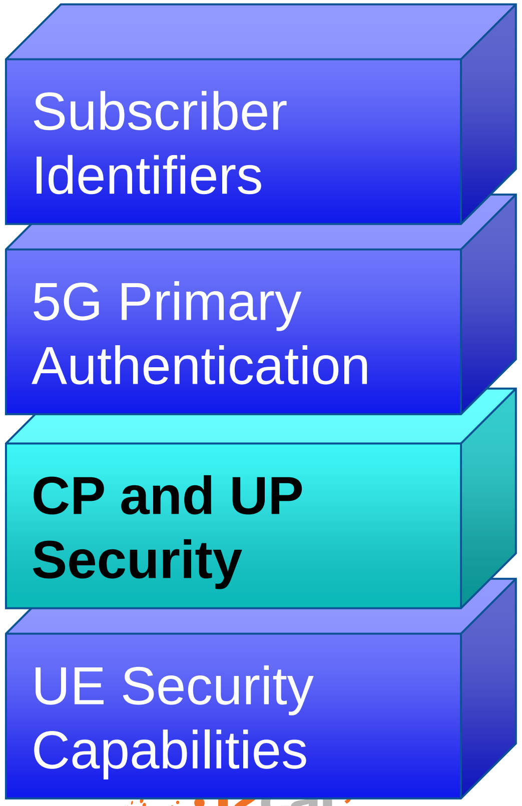


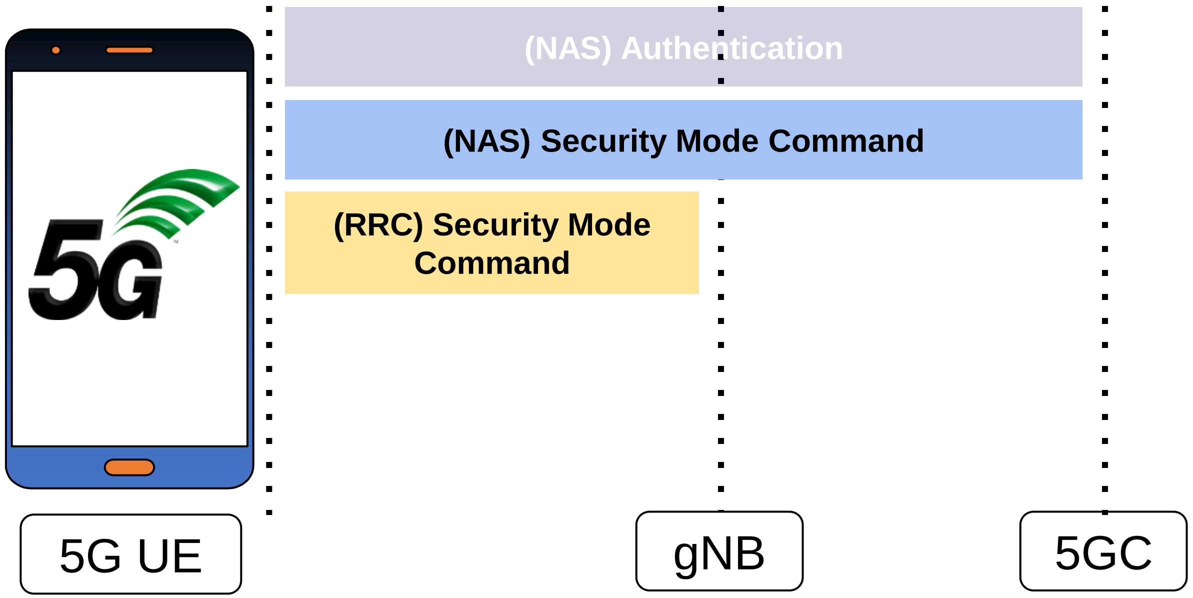
	5G SA	5G NSA
Confidentiality	NEA	EEA
Integrity	NIA	EIA

Enhancements:

5G New Algorithms **NIA** and **NEA**

5G Security Enhancements



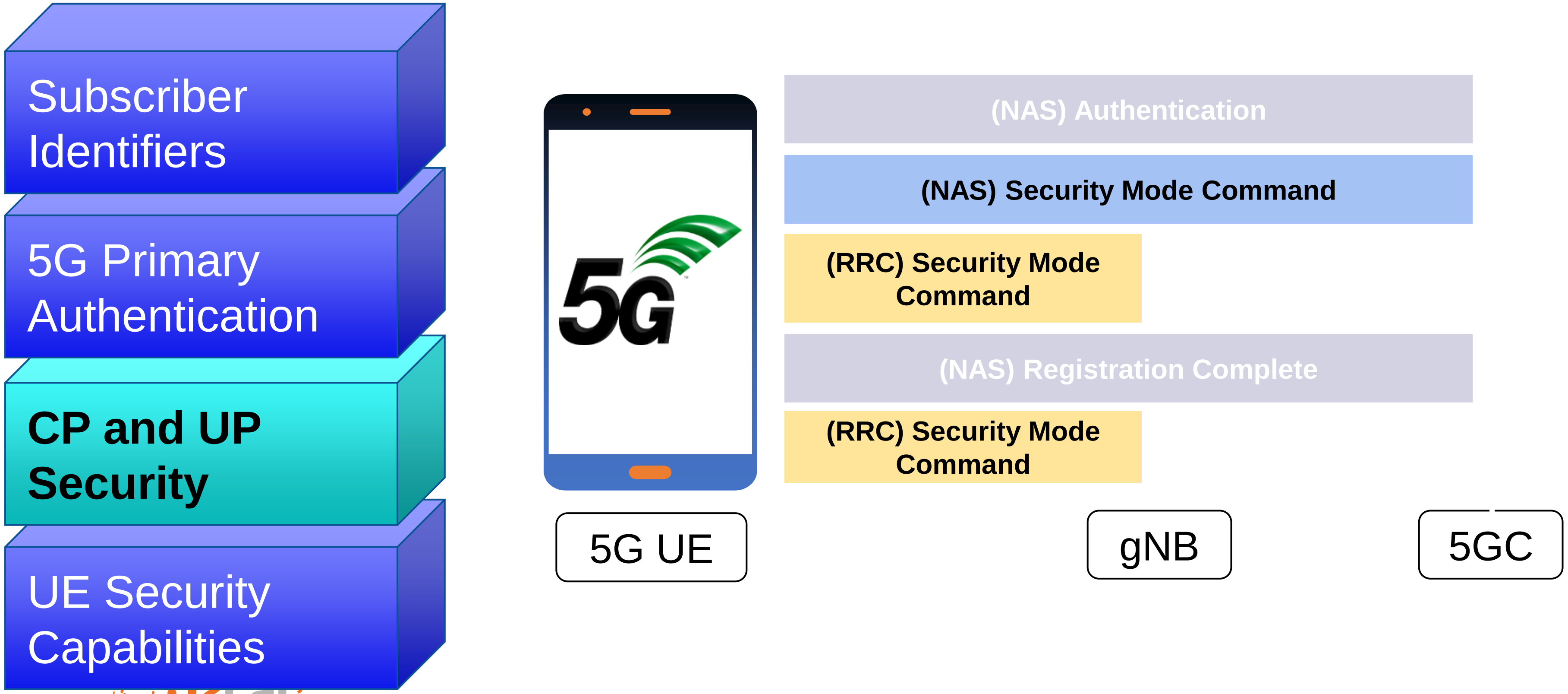


Enhancements:

5G New Algorithms **NIA** and **NEA**

Adding mandatory **confidentiality protection** to initial **NAS** messages

5G Security Enhancements



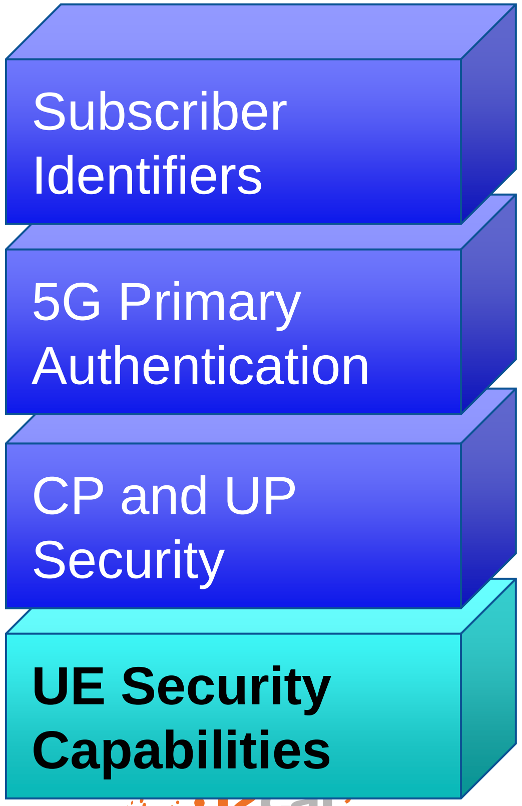
Enhancements:

5G New Algorithms **NIA** and **NEA**

Adding mandatory **confidentiality protection** to initial **NAS** messages

Mandatory algorithms support for **integrity protect UP** data

5G Security Enhancements



	Confidentiality	Integrity
5G SA	NIA	NEA
4G and 5G NSA	EIA	EEA
3G	UIA	UEA

Enhancements:

5G New Algorithms **NIA** and **NEA**

Adding mandatory **confidentiality protection** to initial **NAS** messages

5G Analysis Tools

Commercial and Open-source

4G and 5G Analysis Tools

Commercial Protocol Analysers

Costly software license
Make use of regular **SIM cards**
Network Analysis within the **UE sight**

4G and 5G Analysis Tools

Commercial Protocol Analysers

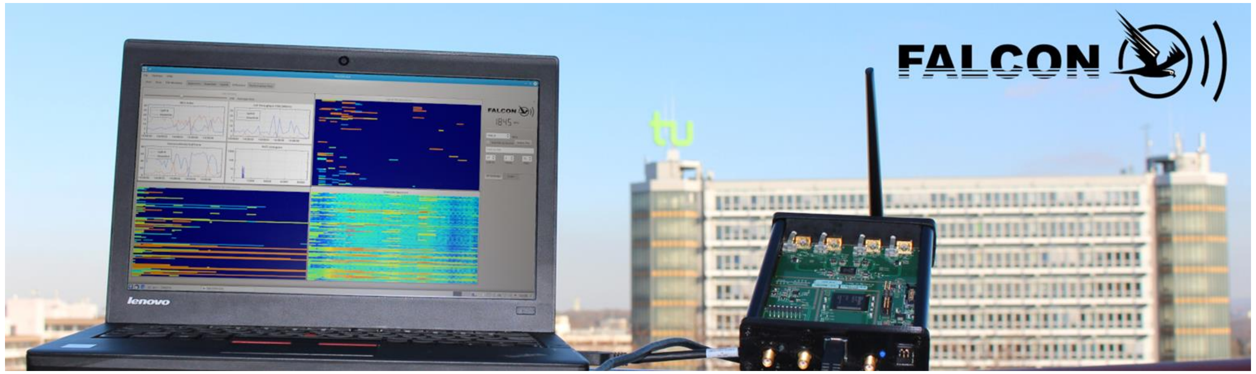
Costly software license
Make use of regular **SIM cards**
Network Analysis within the **UE sight**

KEYSIGHT TECHNOLOGIES
DingLicom
Powering Network Experience

SRSRAN
OPEN AIR INTERFACE

Open Source Protocol Analysers

4G and **5G** support
No 5G Protocol Analyser **Implementations**
Free availability, redistribution and modification
Radio Link Analysis (Both Uplink and Downlink)
SDR based



5G Security In the Wild

Reality Versus Expectations

European 5G Security in the Wild: Reality versus Expectations

Oscar Lasierra
oscar.lasierra@i2cat.net
i2CAT Foundation

Gines Garcia-Aviles
gines.garcia@i2cat.net
i2CAT Foundation

Esteban Municio
esteban.municio@i2cat.net
i2CAT Foundation

Antonio Skarmeta
skarmeta@um.es
University of Murcia

Xavier Costa-Pérez
xavier.costa@i2cat.net
i2CAT Foundation and ICREA
NEC Laboratories Europe

ABSTRACT

5G cellular systems are slowly being deployed worldwide delivering the promised unprecedented levels of throughput and latency to hundreds of millions of users. At such scale security is crucial, and consequently, the 5G standard includes a new series of features to improve the security of its predecessors (i.e., 3G and 4G). In this work, we evaluate the actual deployment in practice of the promised 5G security features by analysing current commercial 5G networks from several European operators. By collecting 5G signalling traffic in the wild in several cities in Spain, we i) fact-check which 5G security enhancements are actually implemented in current deployments, ii) provide a rich overview of the implementation status of each 5G security feature in a wide range of 5G commercial networks in Europe and compare it with previous results in China, iii) analyse the implications of optional features not being deployed, and iv) discuss on the still remaining 4G-inherited vulnerabilities. Our results show that in European 5G commercial networks, the deployment of the 5G security features is still on the works. This is well aligned with results previously reported from China [16] and keeps these networks vulnerable to some 4G attacks, during their migration period from 4G to 5G.

1 INTRODUCTION

The arrival of the fifth generation of mobile networks (5G) is substantially changing the way networks are designed and deployed. From the subscribers perspective, 5G effectively provides an improved performance compared with their predecessors, increasing available bandwidth (e.g., to provide on-demand high-quality video services) and reducing end-to-end latency (e.g., to provide real-time augmented/virtual reality applications). By the end of 2021, more than 176 commercial 5G networks have been deployed worldwide, of which only 22 were already 5G Stand Alone (SA) networks. [11]. Unfortunately, such growing figures also bring greater risks in terms of security.

However, unlike previous mobile generations such as 3G/4G which are subject to a number of known attacks [13, 15, 21, 22], 5G provides security enhancements through a series of new generation specifications defined by the 3rd Generation Partnership Project (3GPP), including TS 33.501 [3] and TS 33.511 [1]. Despite this, while current real-world 5G deployments follow the same architectural security framework reference, neither all of them implement the same 5G security mechanisms enabled by the new specifications, nor they do it in the same way. This is usually caused by the

- O. Lasierra, G. Garcia-Aviles, E. Municio, A. Skarmeta, and X. Costa-Pérez, *"European 5G Security in the Wild: Reality versus Expectations",* In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23). https://doi.org/10.1145/3558482.3581776 https://dl.acm.org/doi/abs/10.1145/3558482.3581776

- O. Lasierra, N. Ludant, G. Garcia-Aviles, E. Municio, G. Noubir, A. Skarmeta, X. Costa-Pérez, *"Unmasking 5G Security: Bridging the Gap Between Expectations and Reality",* TechRxiv, to be published https://www.techrxiv.org/doi/full/10.36227/techrxiv.172055660.06334898

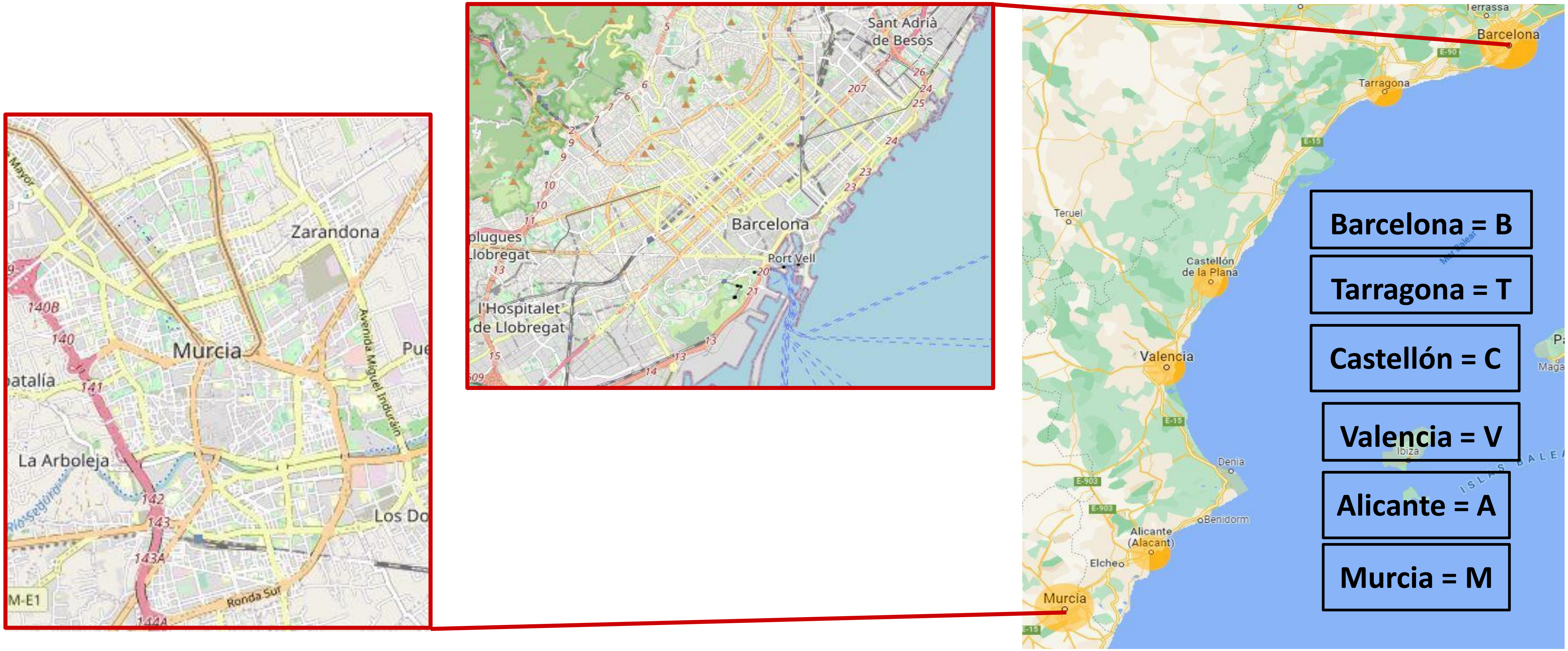
Data Collection

Data Collection

Source			Standard	Commercial											
Operator				Operator A						Operator B					
Location				M	A	V	C	T	B	M	A	V	C	T	B
User Authentication	5G AKA														
	SUCI														
	GUTI Refresh	After Registration													
		After Service Req.													
Confidentiality Protection	NAS Signalling														
	RRC Signalling														
	User Data														
Integrity Protection	NAS Signalling														
	RRC Signalling														
	User Data														
UE Radio	Capabilities Tranfer														
UE Network	Security Capabilities														
Confidentiality Mechanisms	Supported by UE														
Integrity Mechanisms	Supported by UE														

■ 5G SA Mandatory (TS 33.501 [3]) | ■ 5G SA Optional (TS 33.501 [3]) | ■ 5G Compliant | ■ No 5G Compliant

Data collection locations



Data collection locations

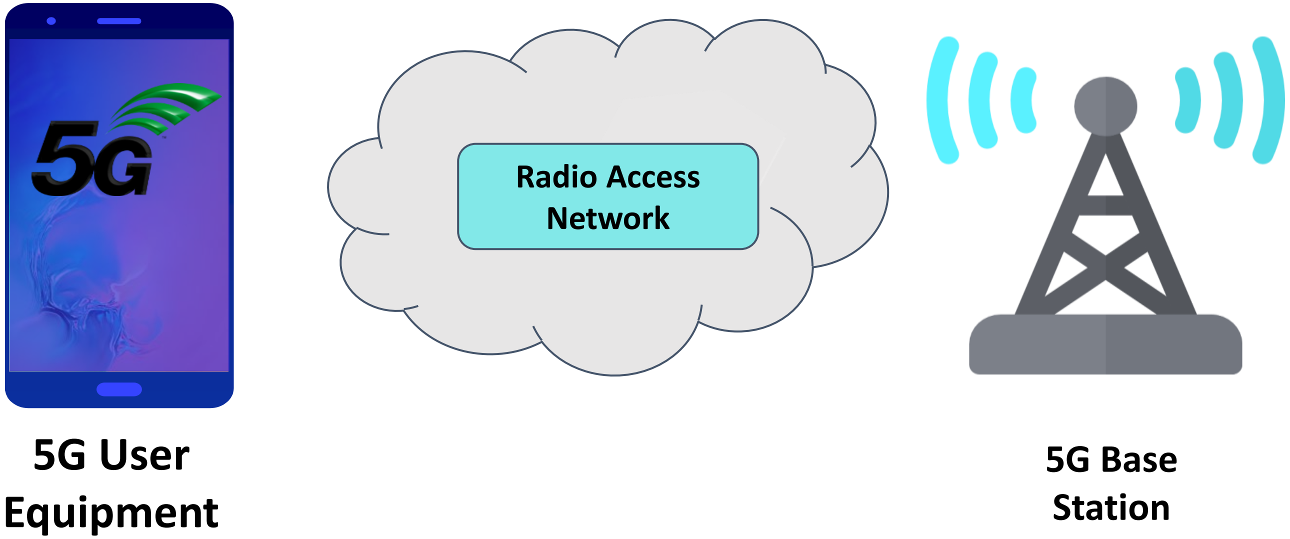
European 5G deployments

- 2 network operators (Operator **A** and **B**)
- **70%** of the countries in the EU
- Same or Similar 5G infrastructure

5G Data Collection methodology

Keysight Nemo Handy Handheld Measurement Solution

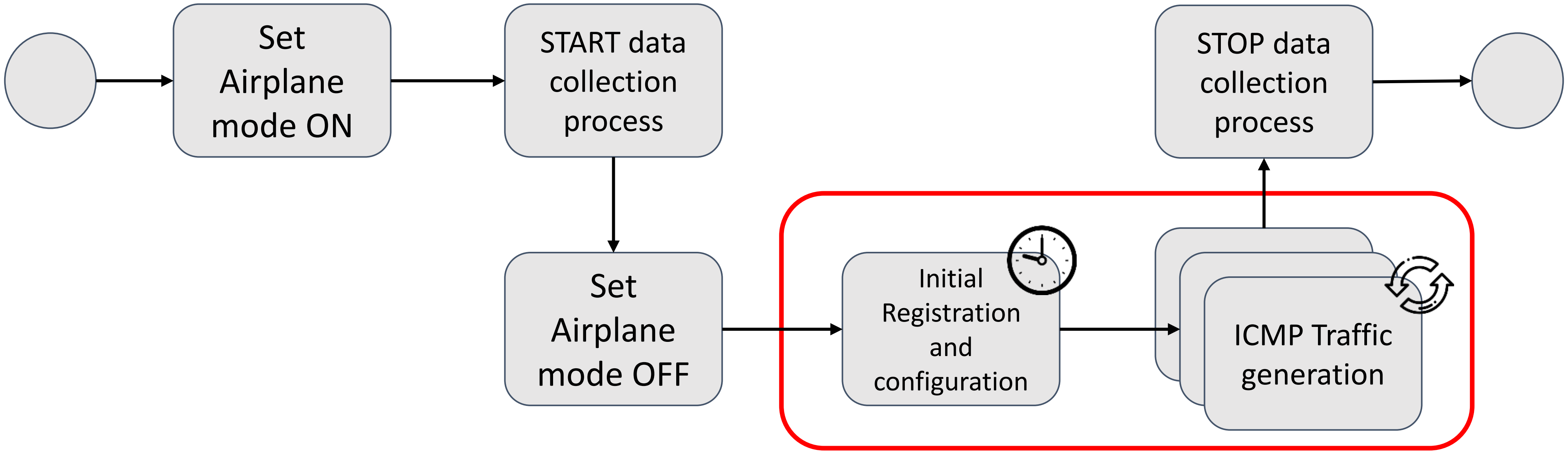
- Android **application**
- Wireless information of **air interface**
- Make use of regular **SIM cards**
- Network Analysis from the **UE side**



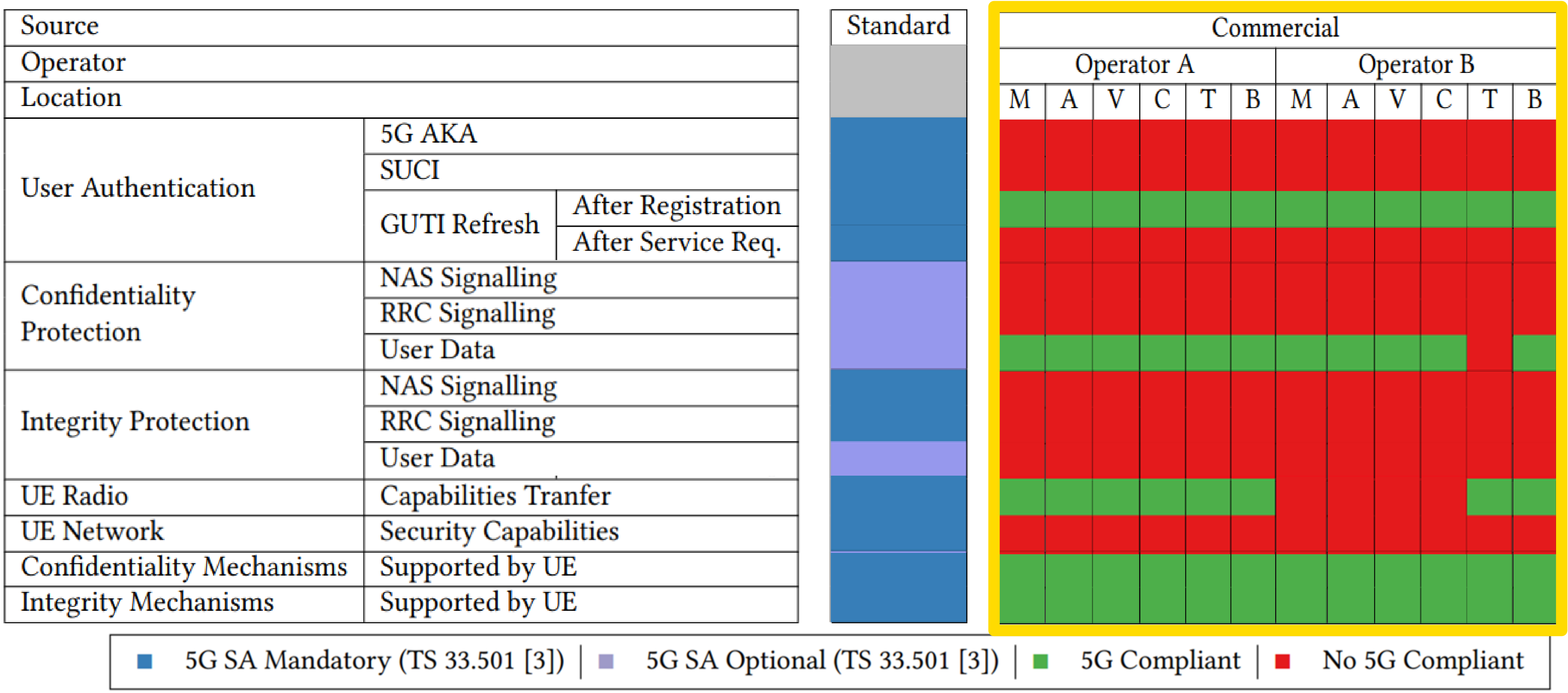
5G Data Collection methodology

Keysight Nemo Handy Handheld Measurement Solution

- Android **application**
- Wireless information of **air interface**
- Make use of regular **SIM cards**
- Network Analysis from the **UE side**

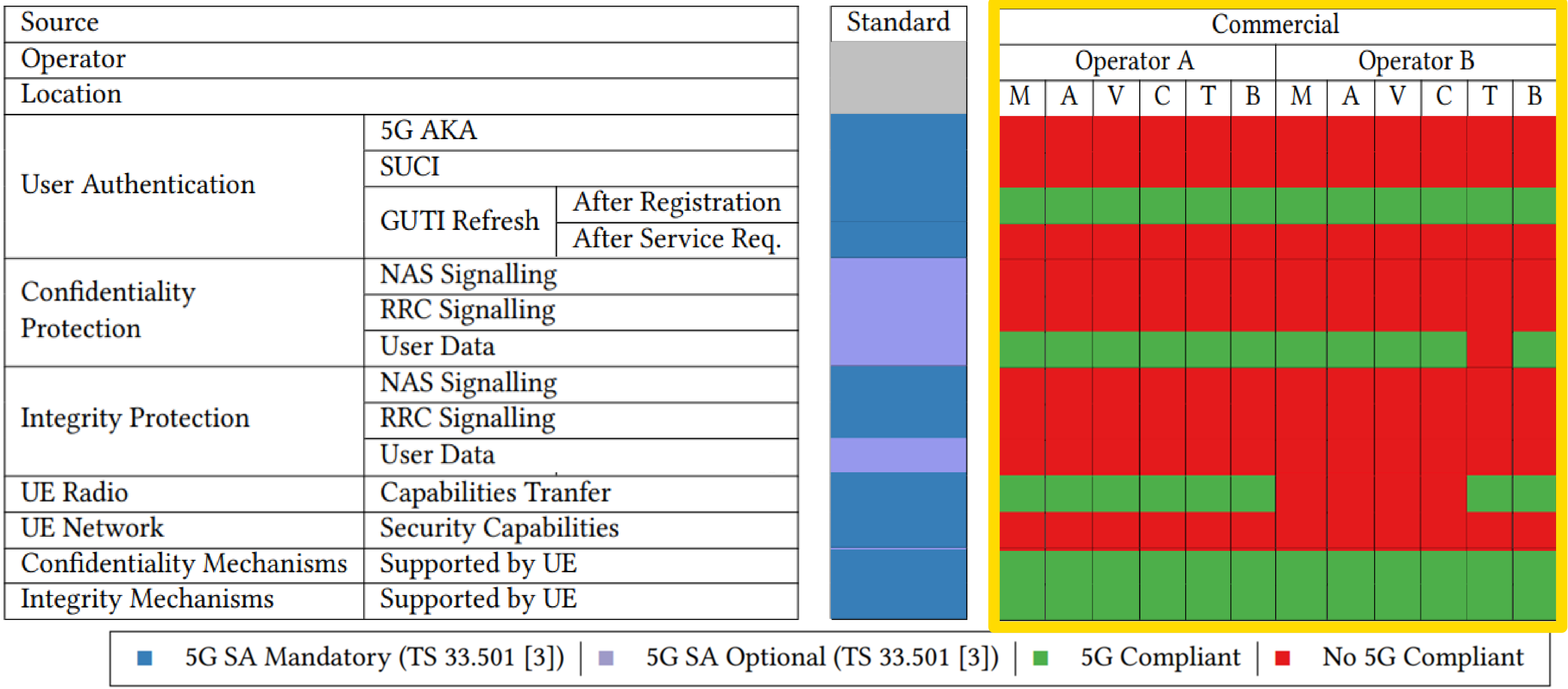


Security Evaluation



Security Evaluation

None of the mobile networks analyzed are **5G SA**



Security Evaluation

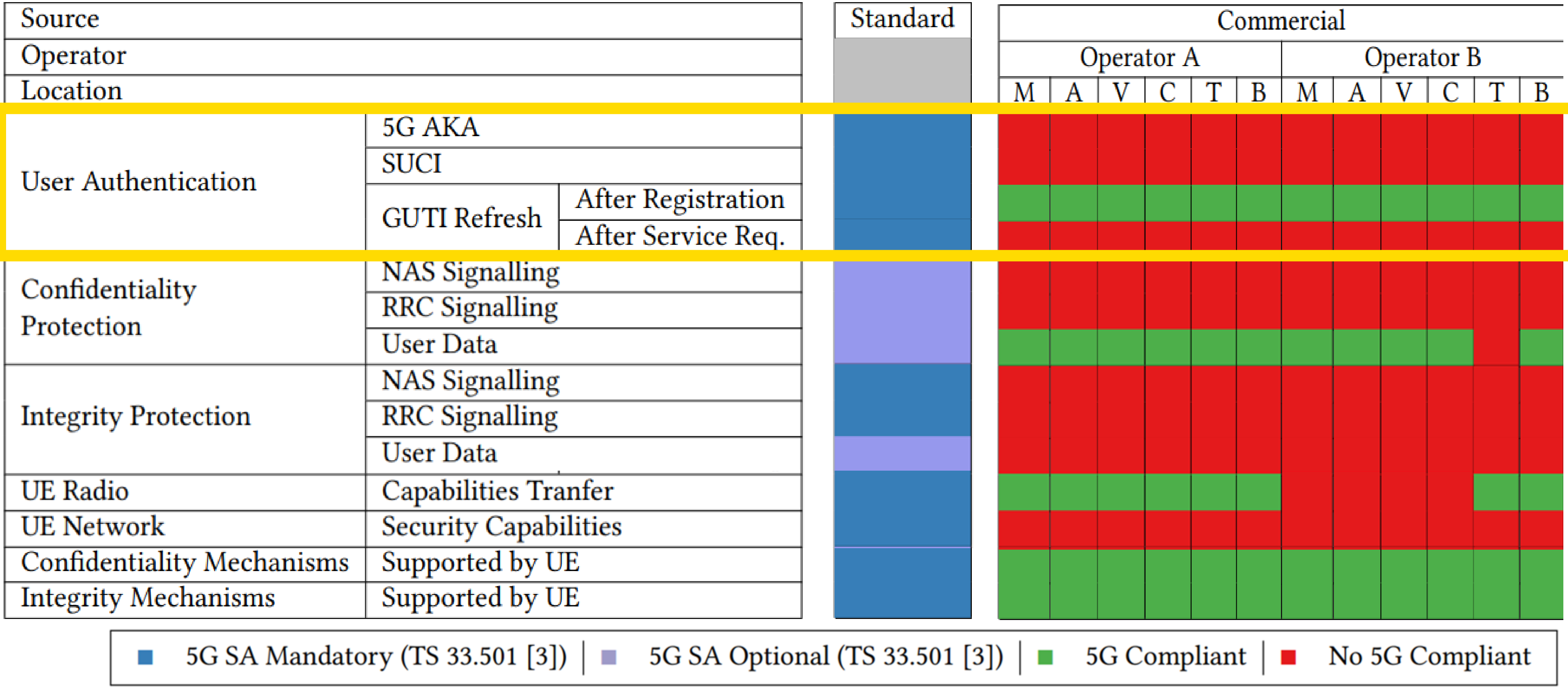
5G Security Features

Source			Standard	Commercial											
Operator				Operator A						Operator B					
Location				M	A	V	C	T	B	M	A	V	C	T	B
User Authentication	5G AKA		Mandatory	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant
	SUCI		Mandatory	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant
	GUTI Refresh	After Registration	Mandatory	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant
		After Service Req.	Mandatory	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant
Confidentiality Protection	NAS Signalling		Optional	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant
	RRC Signalling		Optional	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant
	User Data		Optional	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	No Compliant	Compliant
Integrity Protection	NAS Signalling		Mandatory	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant
	RRC Signalling		Mandatory	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant
	User Data		Optional	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant
UE Radio	Capabilities Tranfer		Mandatory	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	No Compliant	No Compliant	No Compliant	No Compliant	Compliant	Compliant
UE Network	Security Capabilities		Mandatory	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant	No Compliant
Confidentiality Mechanisms	Supported by UE		Mandatory	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant
Integrity Mechanisms	Supported by UE		Mandatory	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant

■ 5G SA Mandatory (TS 33.501 [3]) | ■ 5G SA Optional (TS 33.501 [3]) | ■ 5G Compliant | ■ No 5G Compliant

Security Evaluation

5G Security Features



5G Security Features

SUPI Concealment

- Ciphering Subscriber Permanent Identifiers

5G Authentication

- AKA using new 5G Core Network Functions

5G-GUTI Refresh

- Refresh temporary identifiers after Registration Procedure and Service Request

5G Security Features

SUPI Concealment

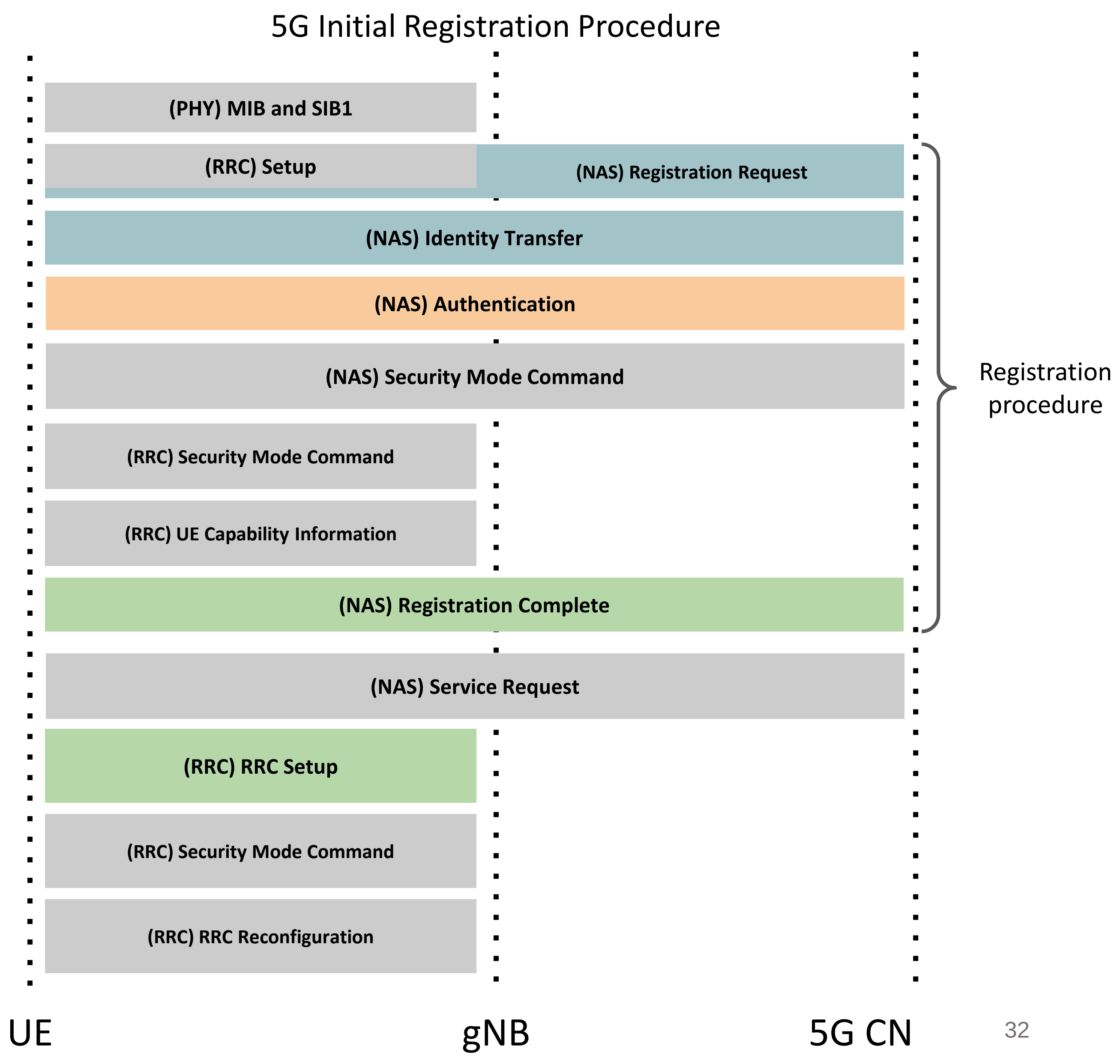
- Ciphering Subscriber Permanent Identifiers

5G Authentication

- AKA using new 5G Core Network Functions

5G-GUTI Refresh

- Refresh temporary identifiers after Registration Procedure and Service Request



5G Security Features

SUPI Concealment

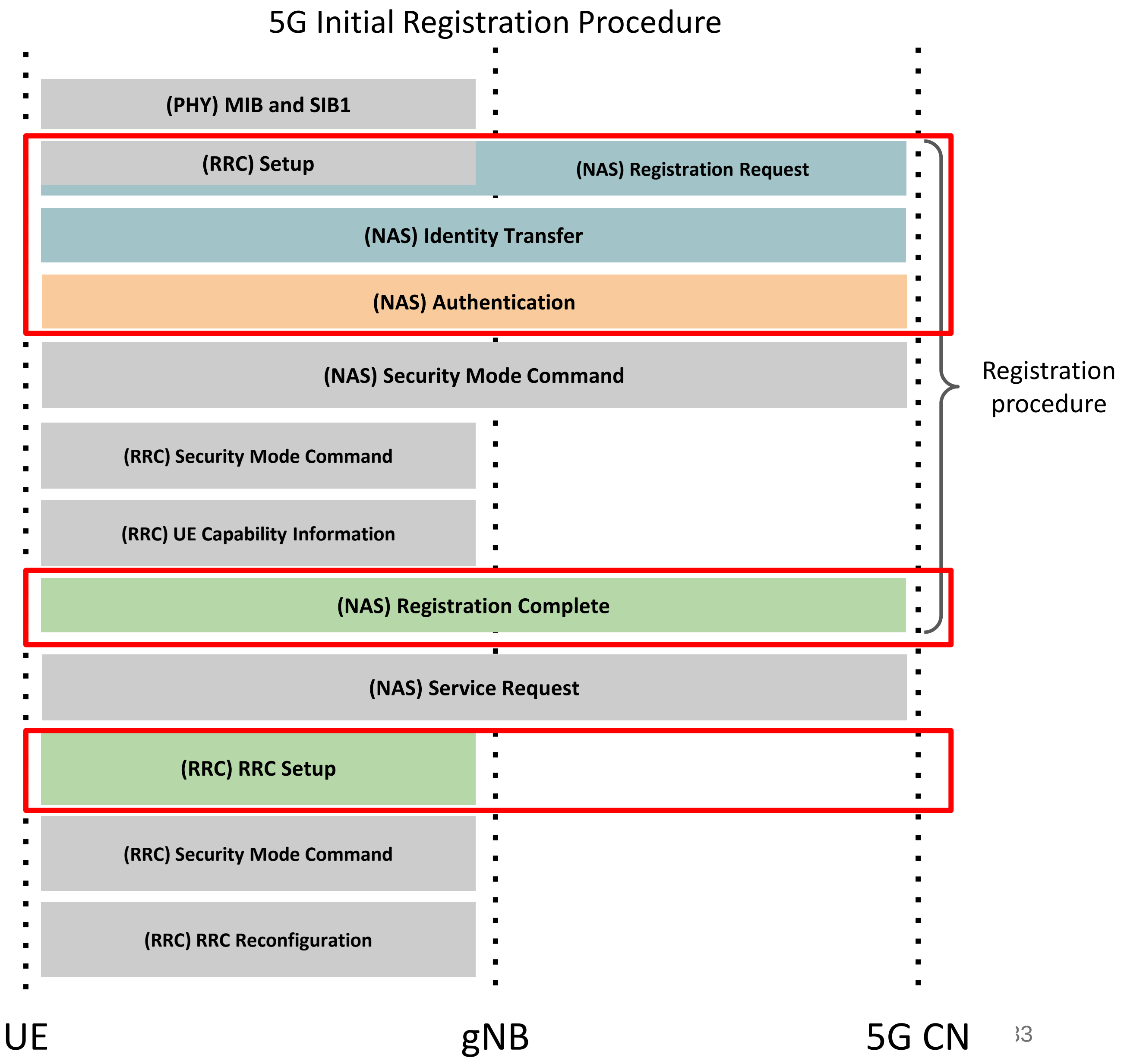
- Ciphering Subscriber Permanent Identifiers

5G Authentication

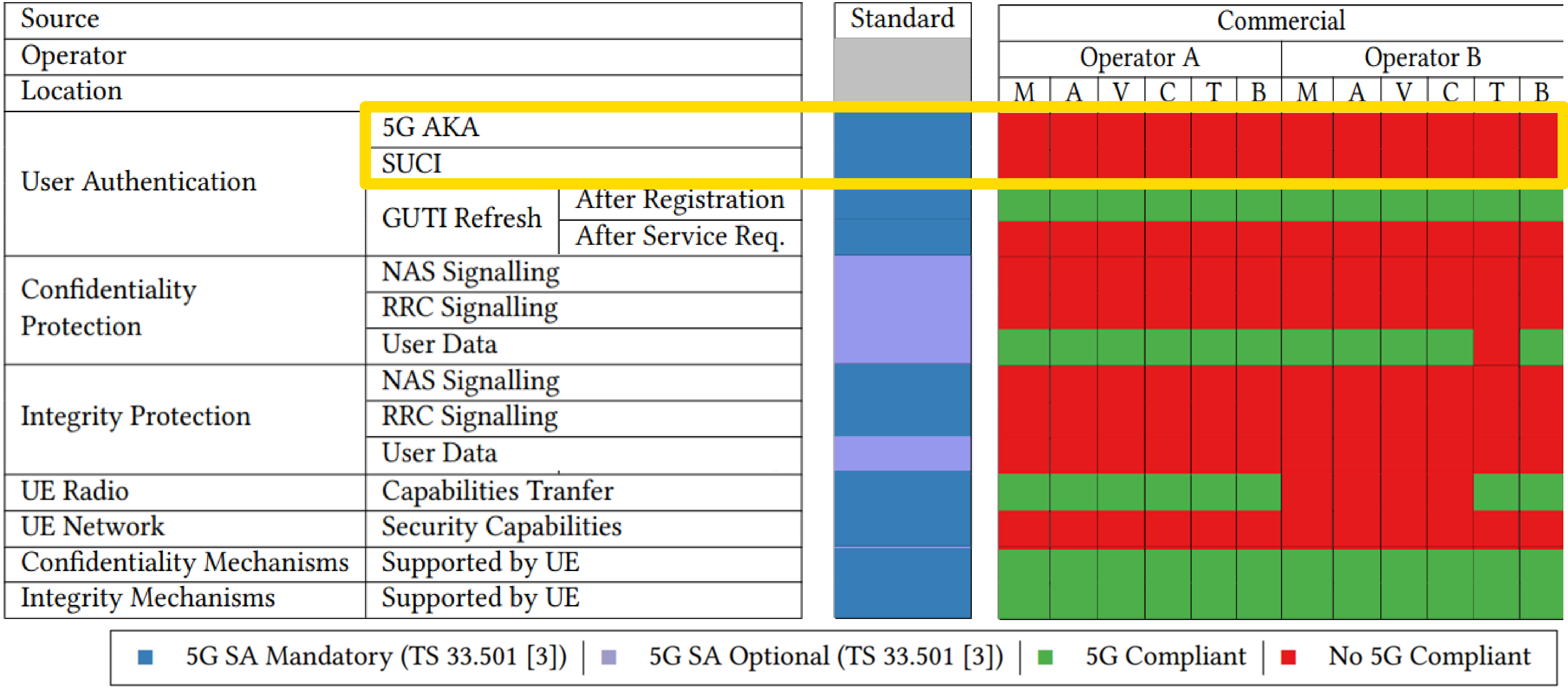
- AKA using new 5G Core Network Functions

5G-GUTI Refresh

- Refresh temporary identifiers after Registration Procedure and Service Request



Security Evaluation



Security Evaluation

Source			Standard	Commercial											
Operator				Operator A						Operator B					
Location				M	A	V	C	T	B	M	A	V	C	T	B
User Authentication	5G AKA		5G SA Mandatory	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant
	SUCI		5G SA Mandatory	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant
	GUTI Refresh	After Registration	5G SA Mandatory	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant
		After Service Req.	5G SA Mandatory	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant
Confidentiality Protection	NAS Signalling		5G SA Optional	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant
	RRC Signalling		5G SA Optional	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant
	User Data		5G SA Optional	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	No 5G Compliant	5G Compliant
Integrity Protection	NAS Signalling		5G SA Mandatory	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant
	RRC Signalling		5G SA Mandatory	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant
	User Data		5G SA Optional	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant
UE Radio	Capabilities Tranfer		5G SA Mandatory	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	5G Compliant	5G Compliant
UE Network	Security Capabilities		5G SA Mandatory	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant	No 5G Compliant
Confidentiality Mechanisms	Supported by UE		5G SA Mandatory	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant
Integrity Mechanisms	Supported by UE		5G SA Mandatory	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant	5G Compliant

■ 5G SA Mandatory (TS 33.501 [3]) | ■ 5G SA Optional (TS 33.501 [3]) | ■ 5G Compliant | ■ No 5G Compliant

5G Security Features

NAS Integrity and Confidentiality

- Protect the initial NAS message

RRC Integrity and Confidentiality

- Protect the Access Stratum Control plane messages

UP Integrity and Confidentiality

- Protect the User traffic data

5G Algorithms expected:

- Confidentiality: 5G - **NEA**
- Integrity: 5G - **NIA**

5G Security Features

NAS Integrity and Confidentiality

- Protect the initial NAS message

RRC Integrity and Confidentiality

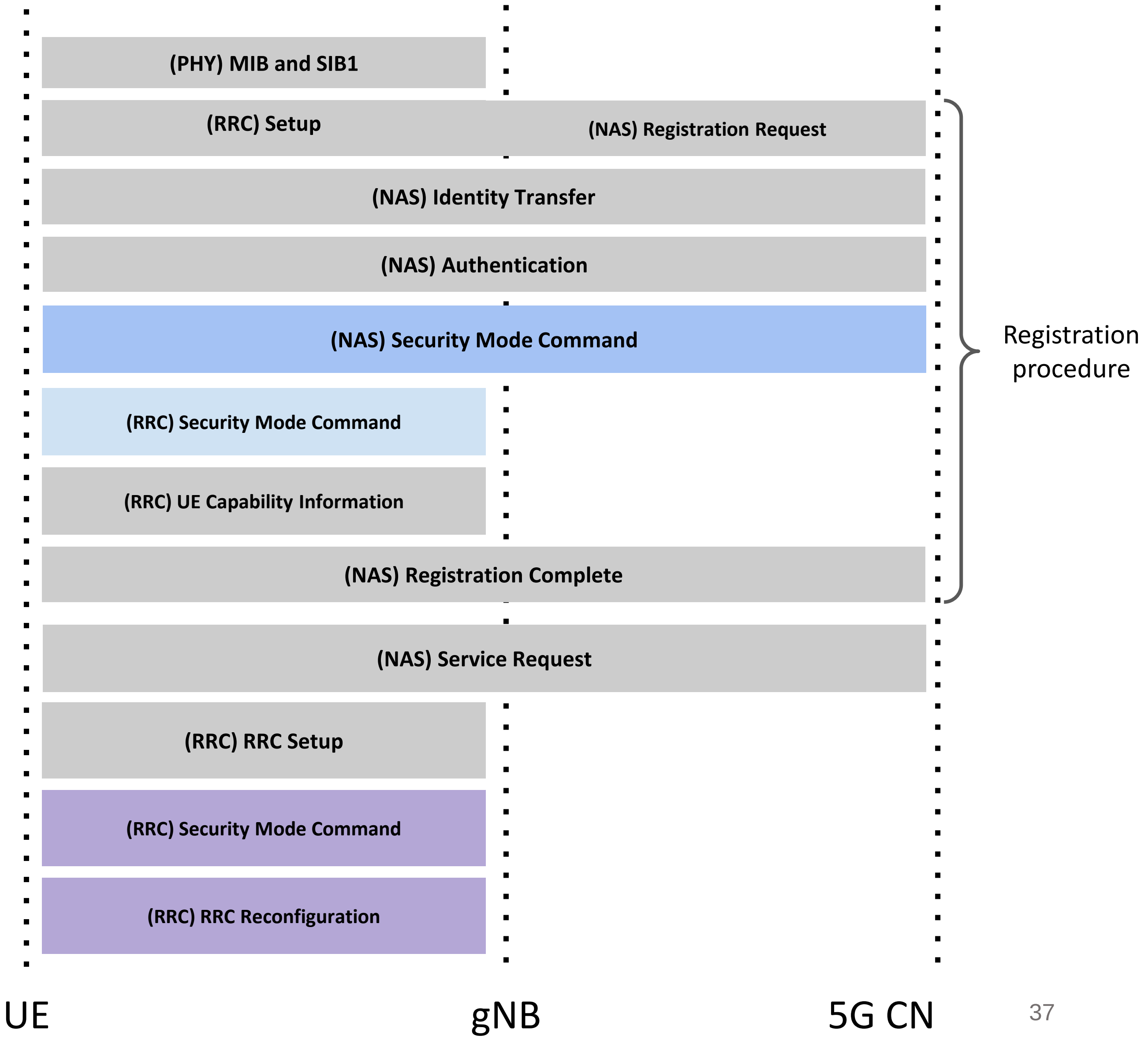
- Protect the Access Stratum Control plane messages

UP Integrity and Confidentiality

- Protect the User traffic data

5G Algorithms expected:
- Confidentiality: 5G - **NEA**
- Integrity: 5G - **NIA**

5G Initial Registration Procedure



5G Security Features

NAS Integrity and Confidentiality

- Protect the initial NAS message

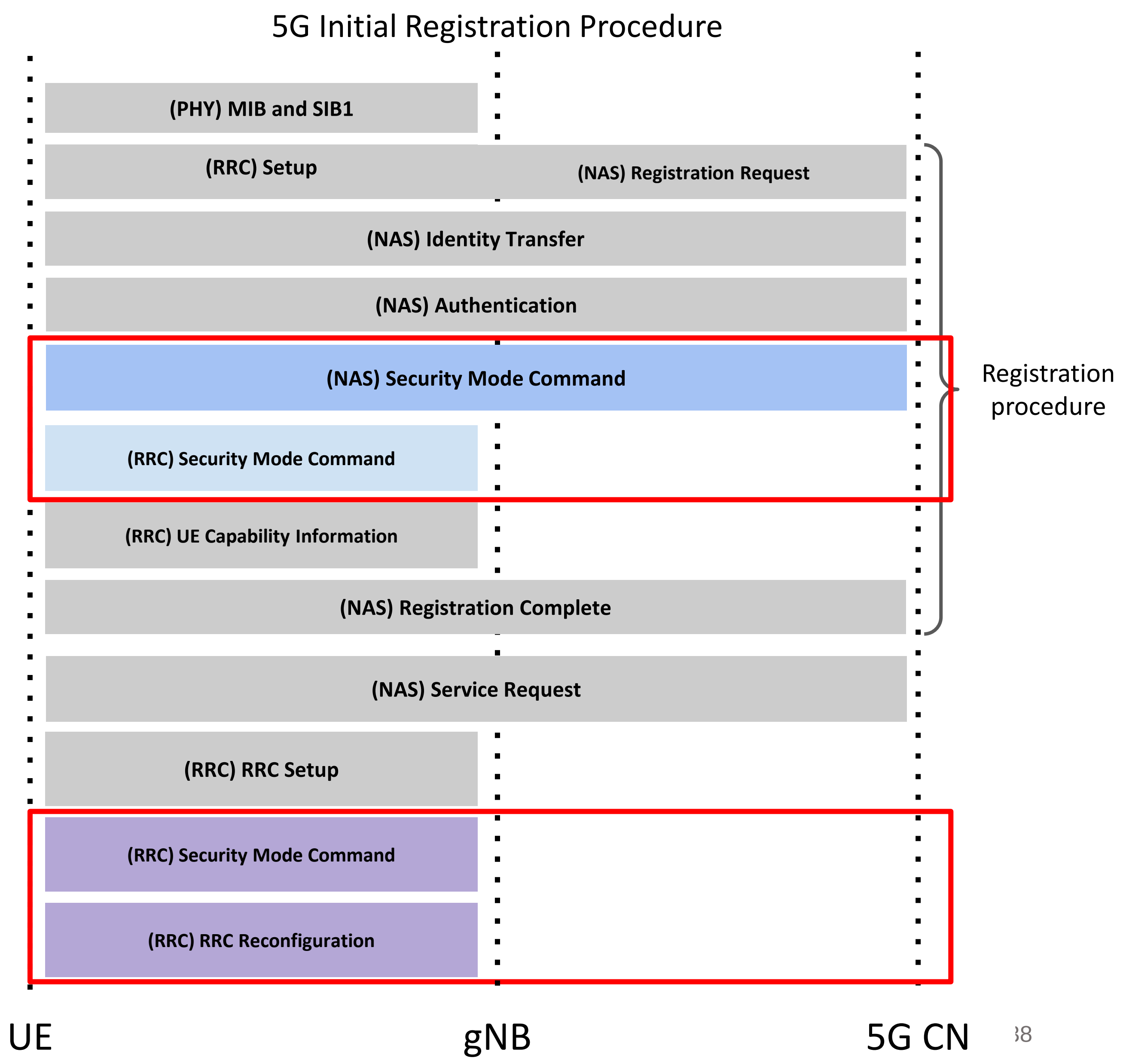
RRC Integrity and Confidentiality

- Protect the Access Stratum Control plane messages

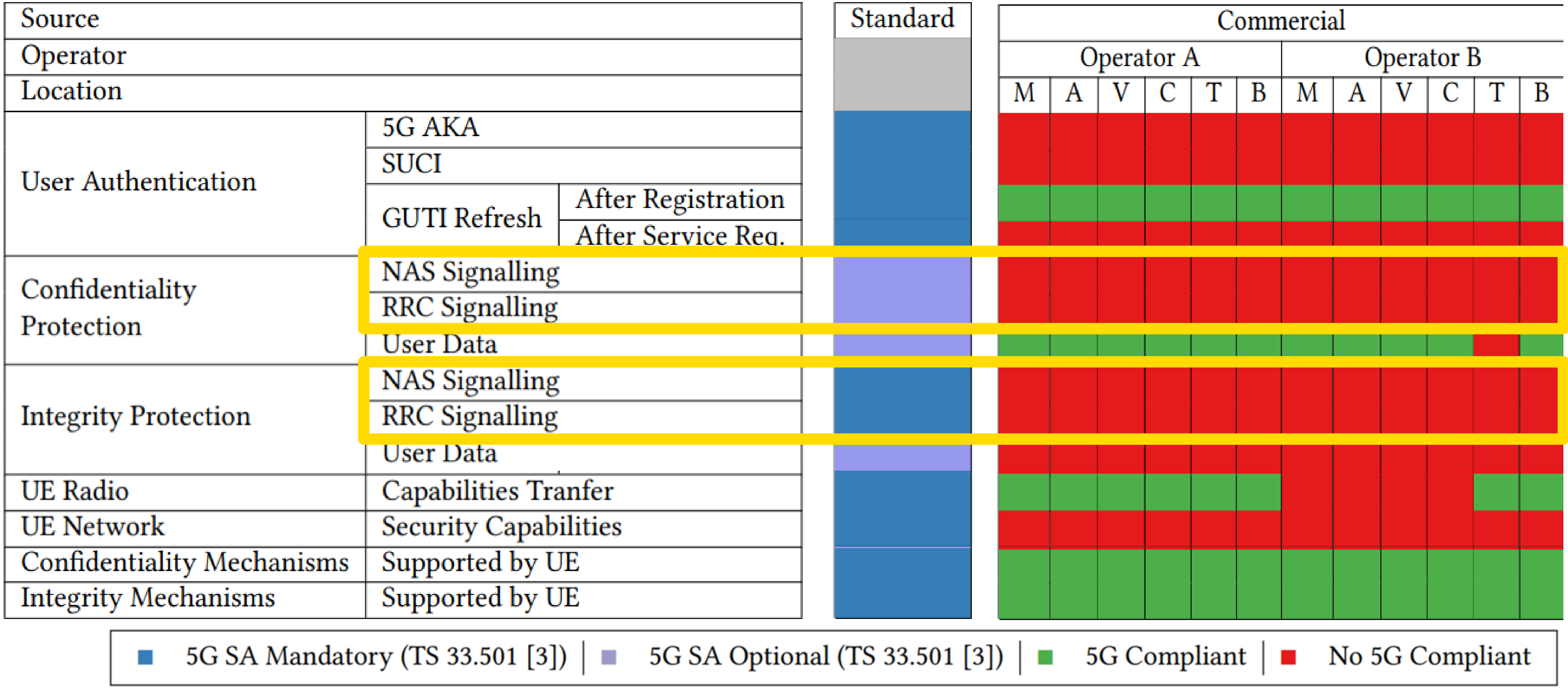
UP Integrity and Confidentiality

- Protect the User traffic data

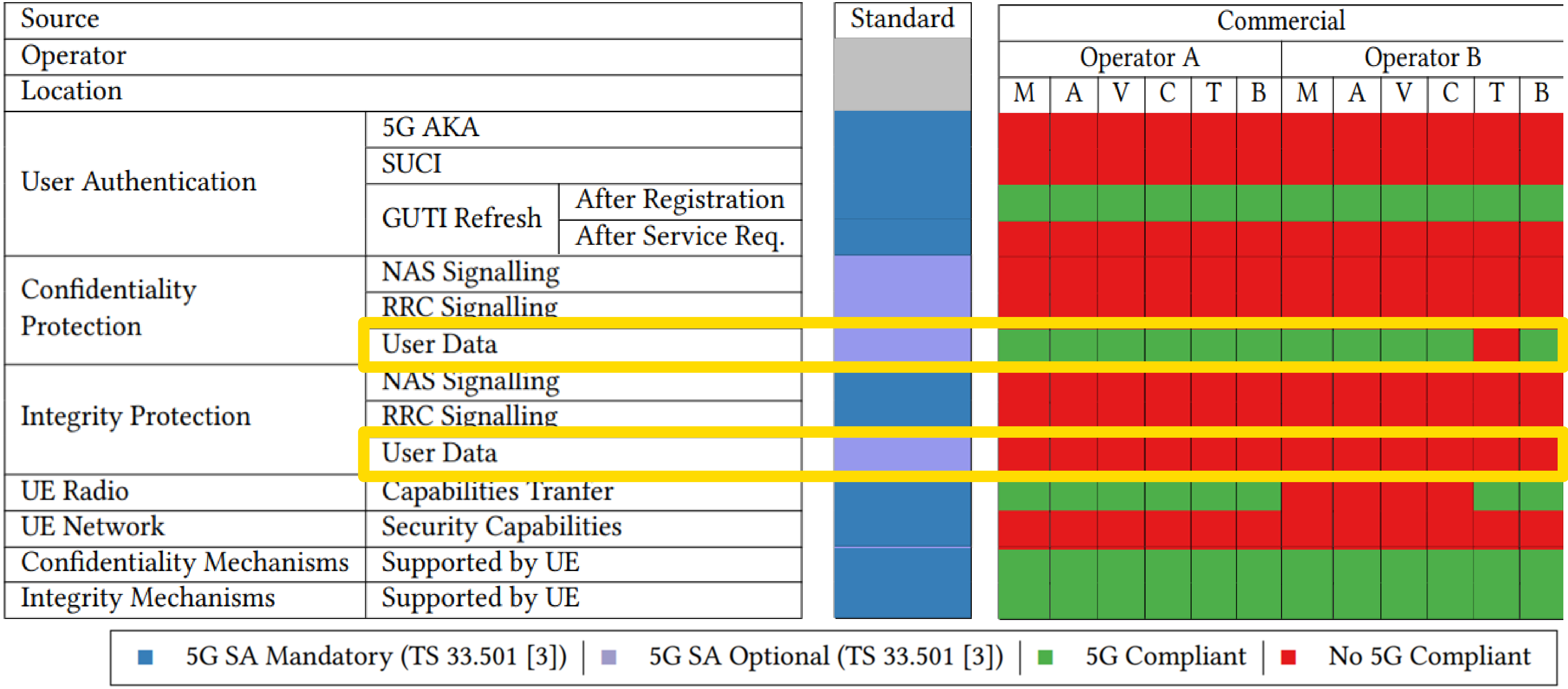
5G Algorithms expected:
- Confidentiality: 5G - **NEA**
- Integrity: 5G - **NIA**



Security Evaluation

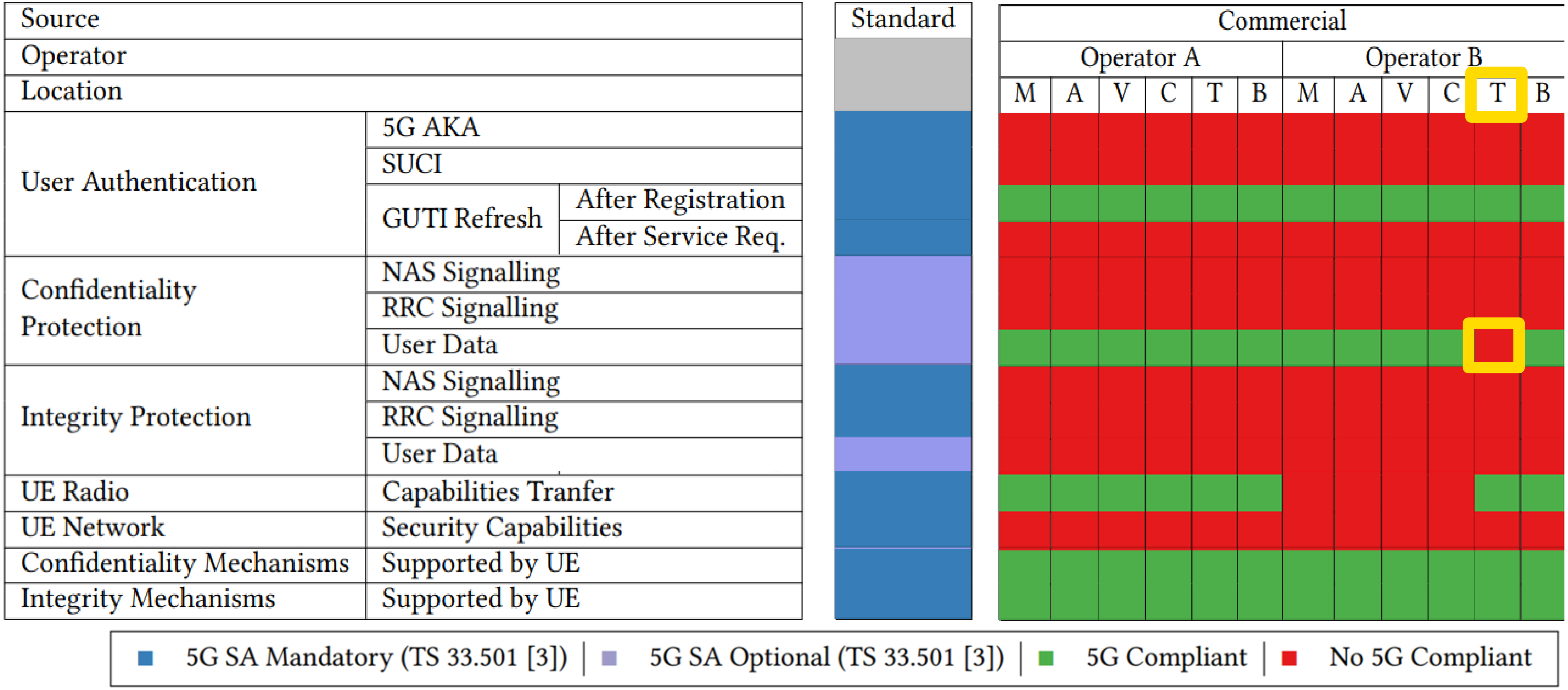


Security Evaluation



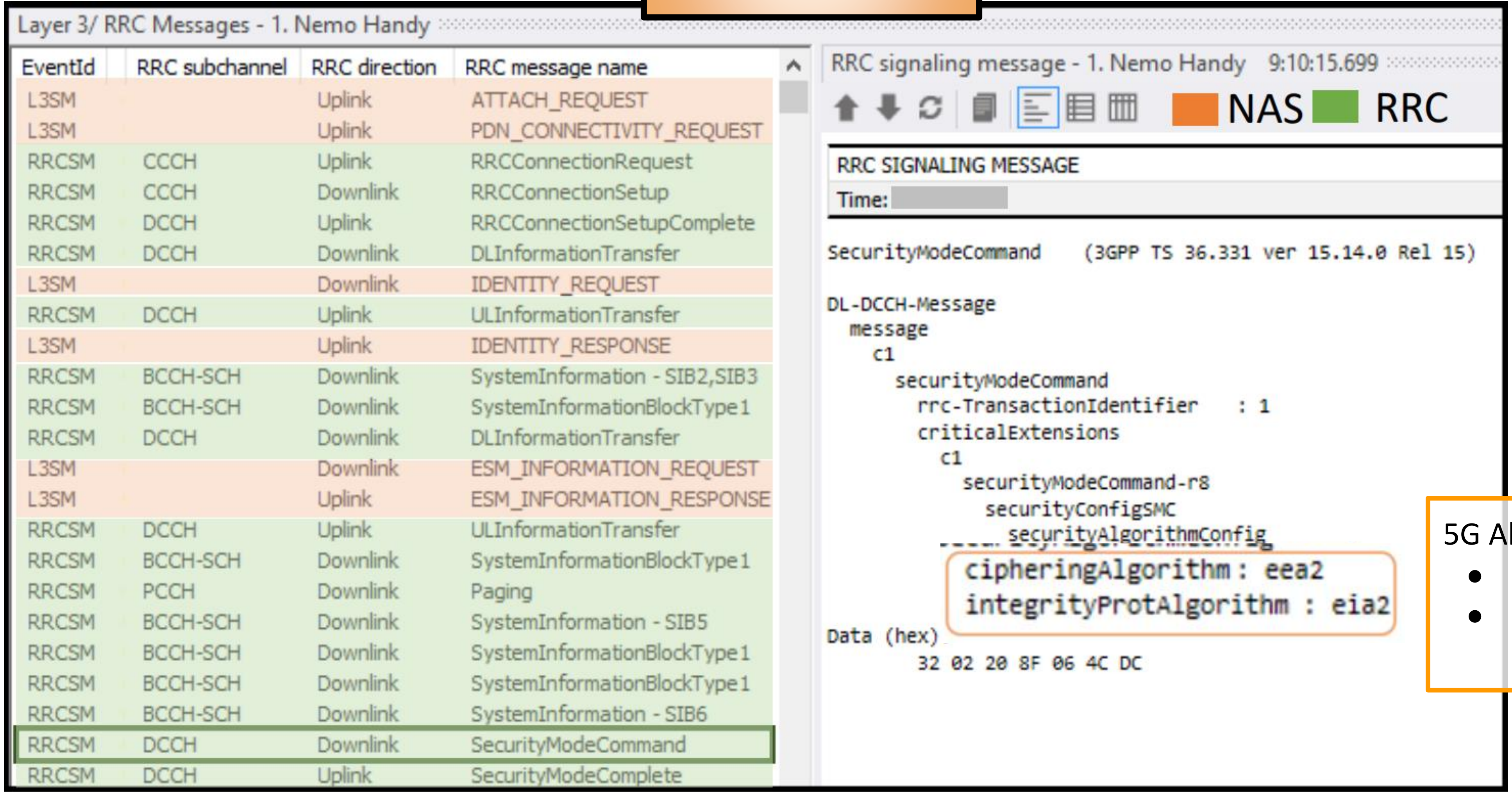
Security Evaluation

Tarragona Operator B
has 4G Deployment



5G Data Analysis

Confidentiality and Integrity



5G Algorithms equivalence:

- nea2
- nia2

5G Security Features

UE Security Capabilities

- Field within initial NAS message
- UE integrity and confidentiality supported algorithms

UE Radio Capabilities

- UE capabilities for radio access
- Send after RRC SMC

5G Security Features

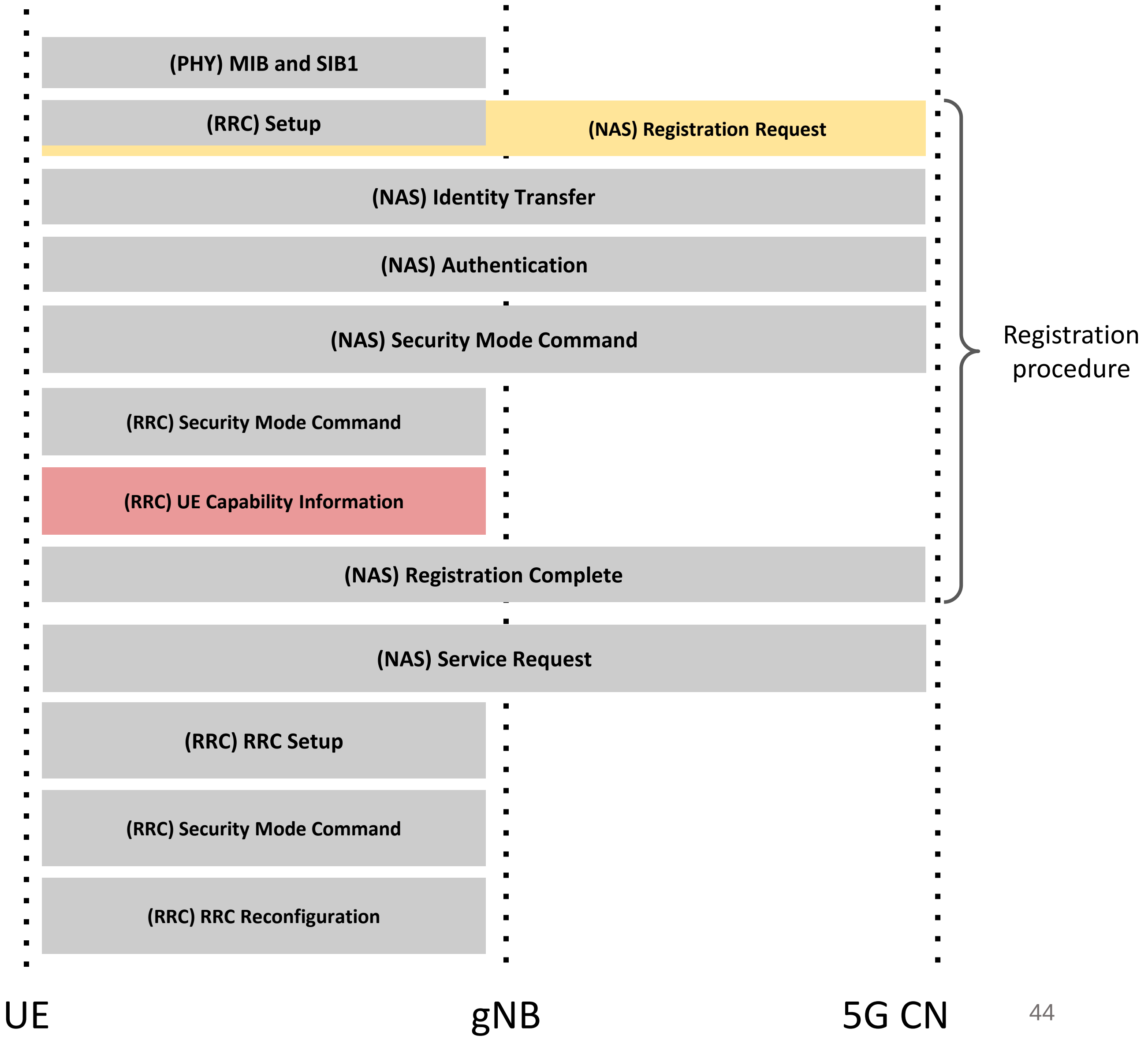
UE Security Capabilities

- Field within initial NAS message
- UE integrity and confidentiality supported algorithms

UE Radio Capabilities

- UE capabilities for radio access
- Send after RRC SMC

5G Initial Registration Procedure



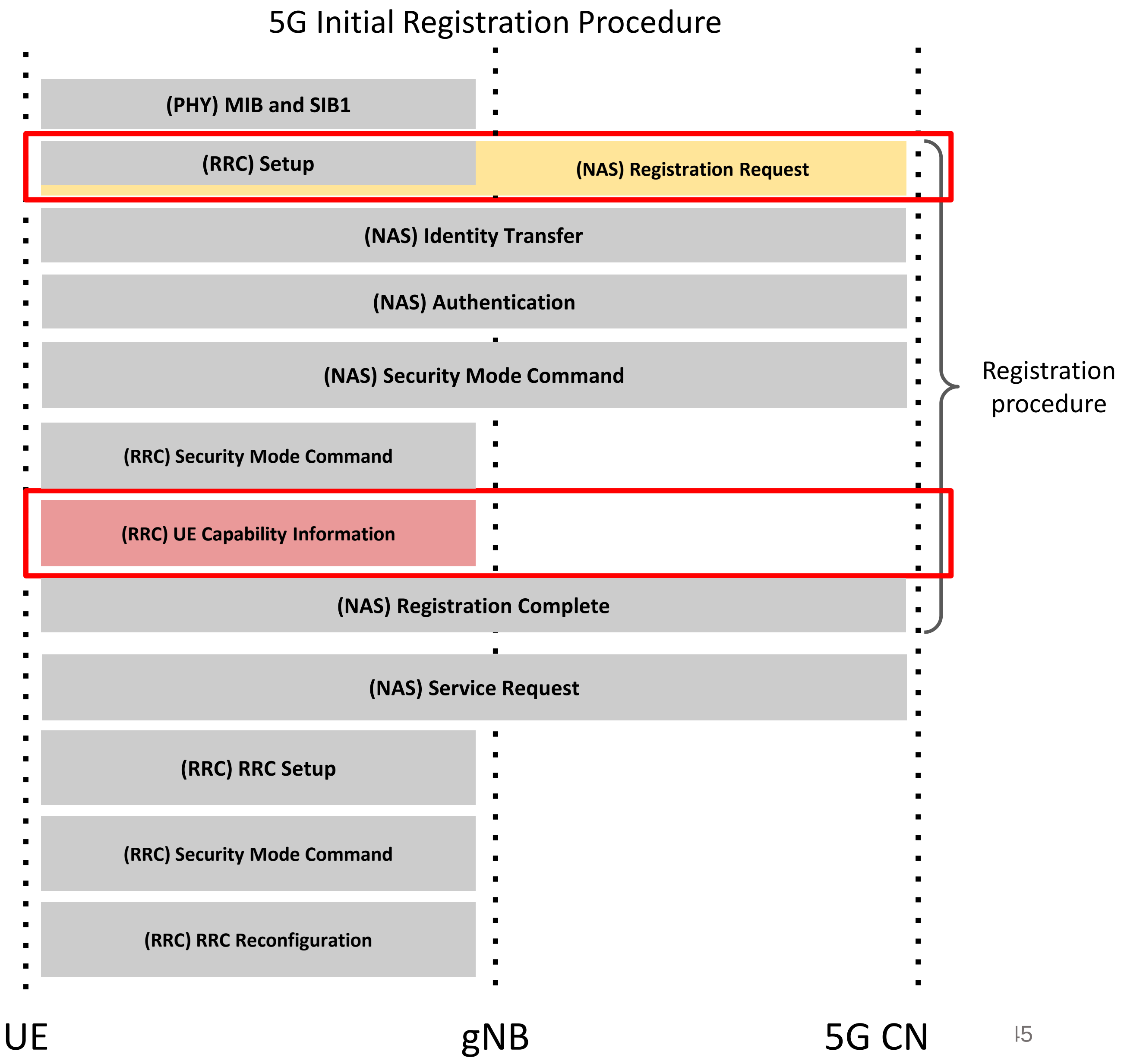
5G Security Features

UE Security Capabilities

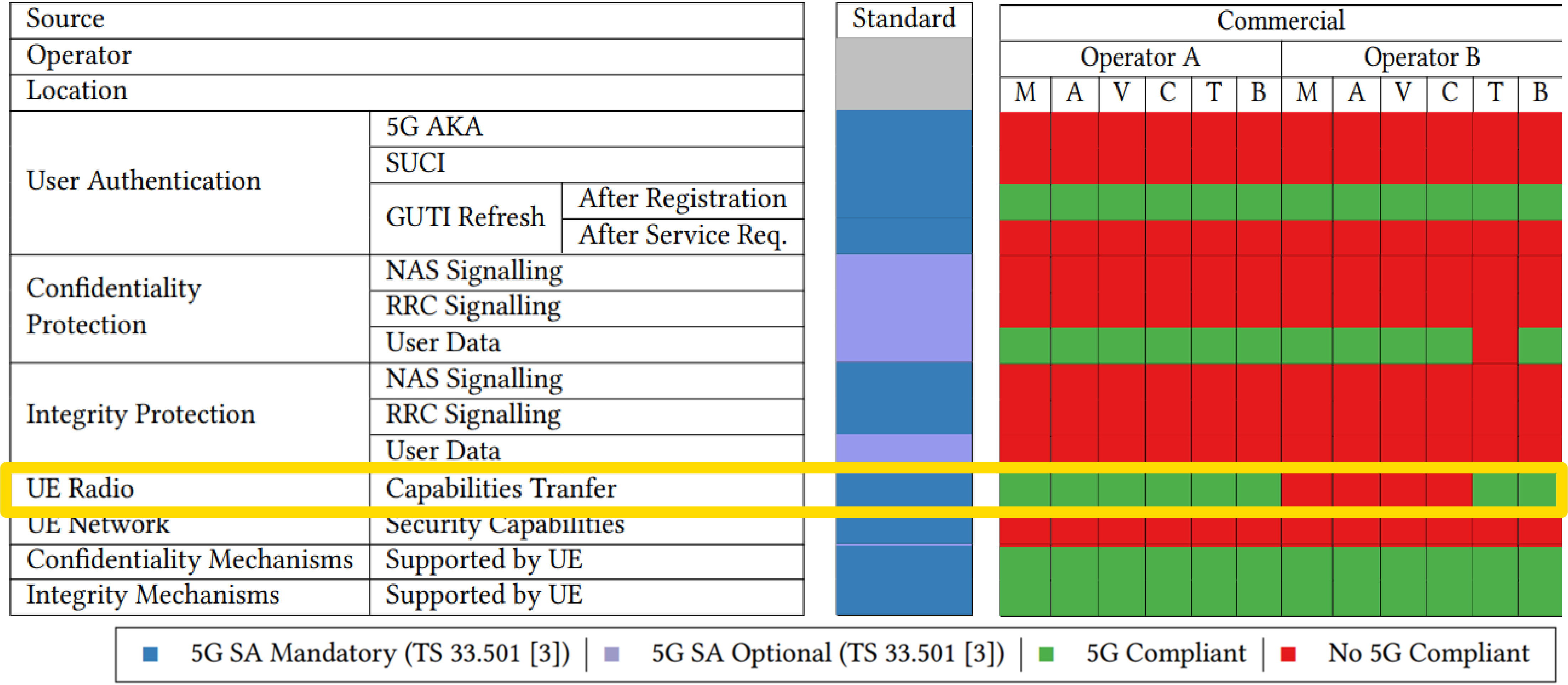
- Field within initial NAS message
- UE integrity and confidentiality supported algorithms

UE Radio Capabilities

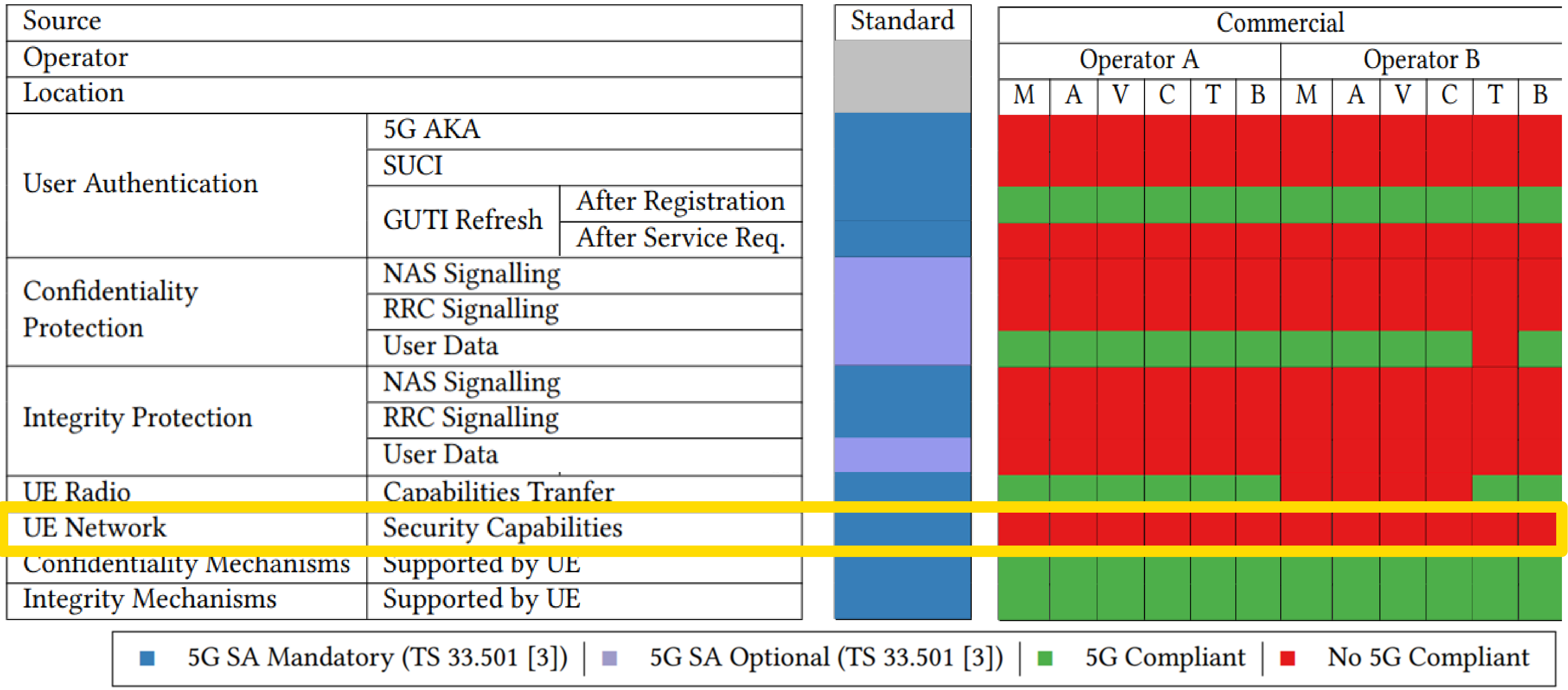
- UE capabilities for radio access
- Send after RRC SMC



Security Evaluation

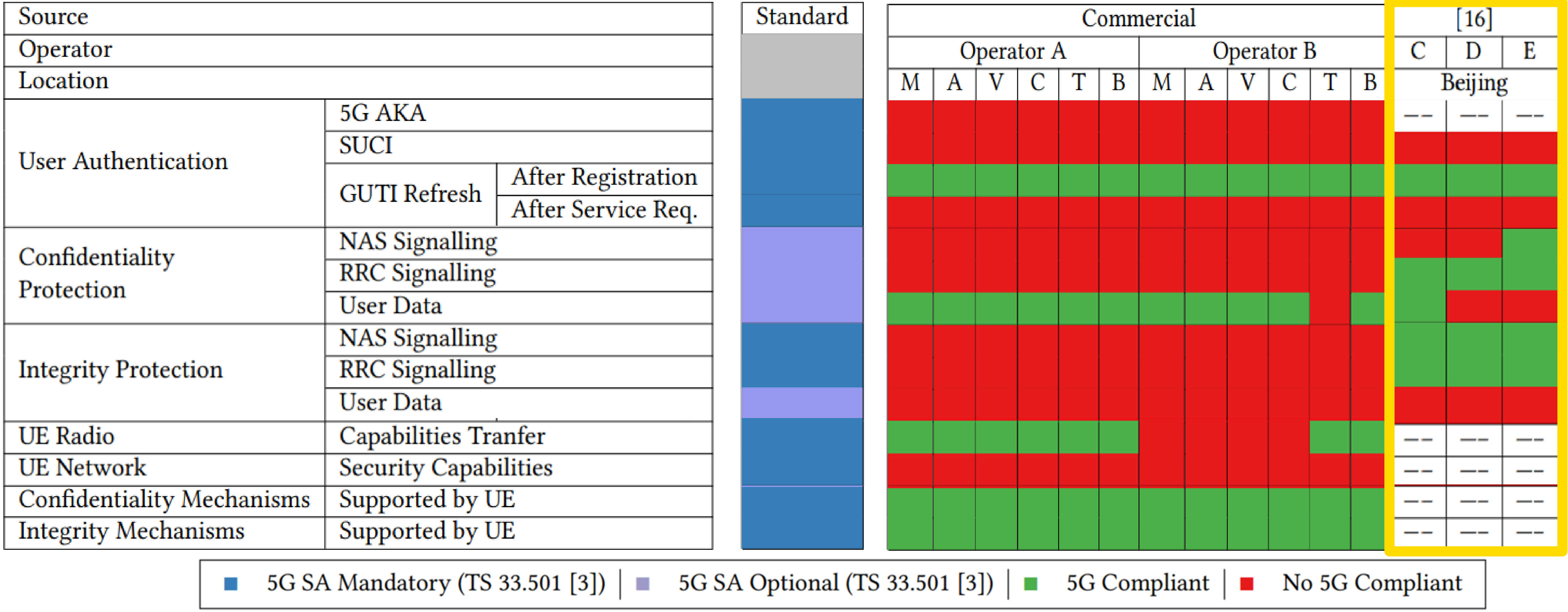


Security Evaluation



Security Evaluation

[16] Shiyue Nie et al. 2022. Measuring the Deployment of 5G Security Enhancement.



Attacks in 5G Commercial Networks

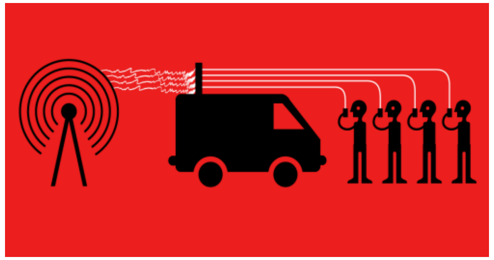
Found Vulnerabilities

- No concealment of permanent identifiers
  No specific policies for GUTI reallocation.
- Lack of randomness and the use of XOR in AUTS
- UP Confidentiality Optional Support
- UP Integrity Optional Support
- Not security transfer of UE Radio Capabilities

Attacks in Actual 5G Commercial Networks

Subscriber Credentials

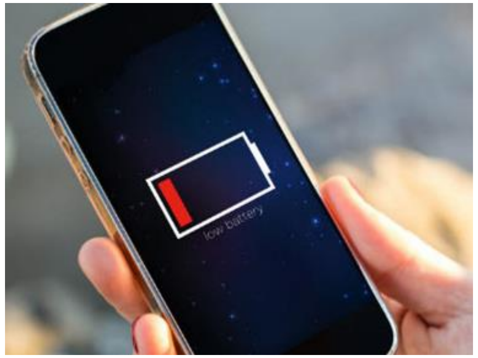
IMSI Catching



Tracking

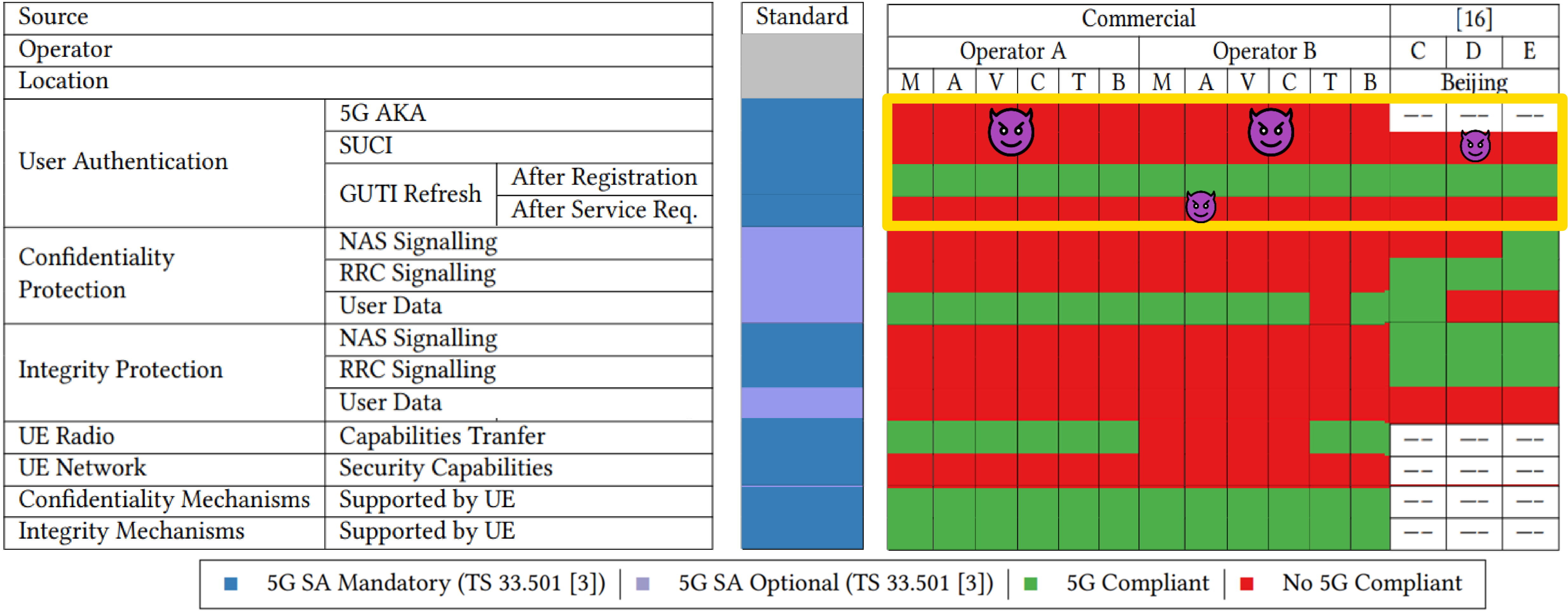
Authentication

Activity Monitoring



Subscriber Credentials Authentication

IMSI Catching
Tracking
Activity Monitoring



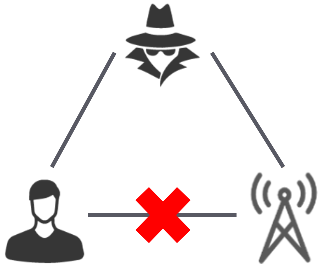
Attacks in Actual 5G Commercial Networks

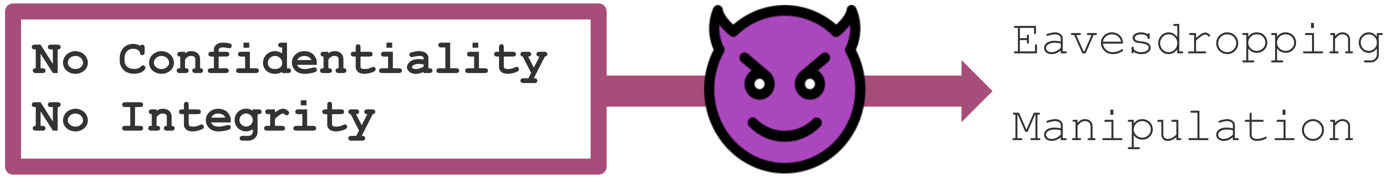
No Confidentiality

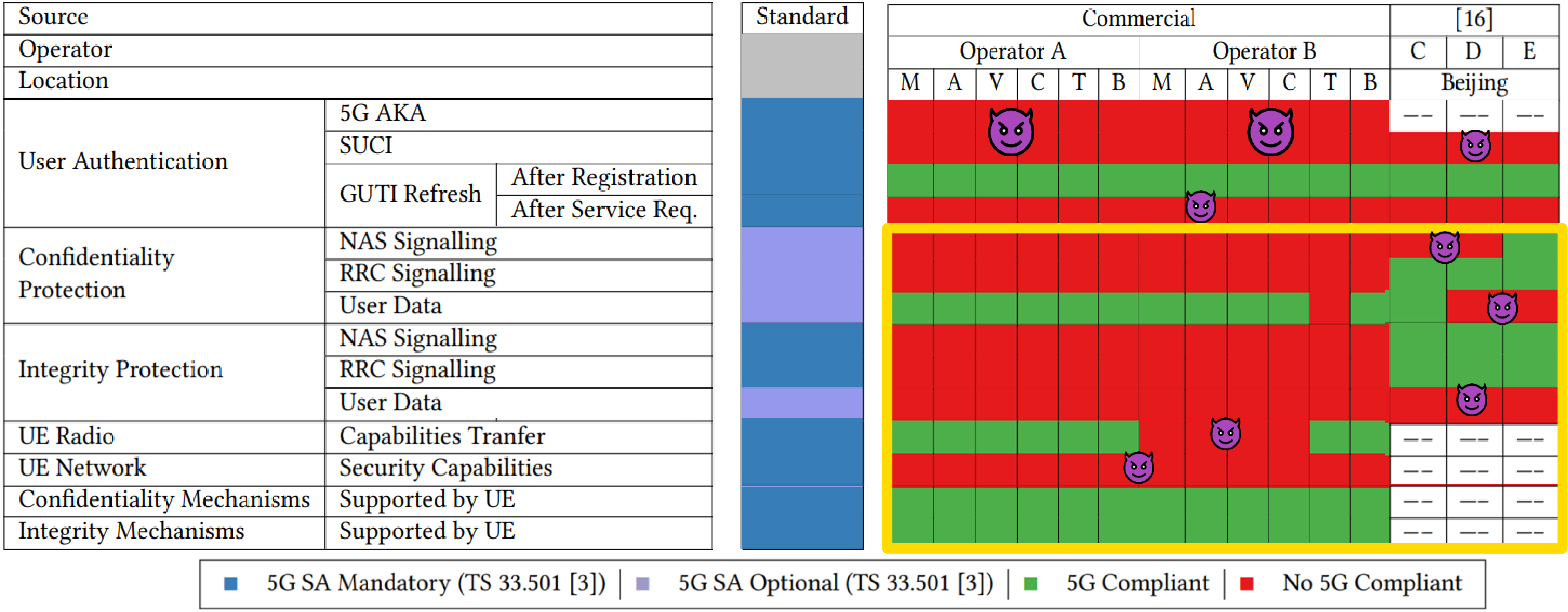
Eavesdropping

No Integrity

Manipulation



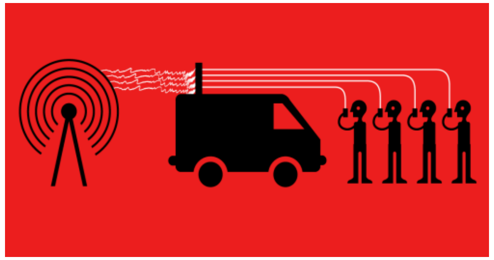

No Confidentiality
No Integrity
Eavesdropping
Manipulation


Source
Operator
Location
User Authentication
5G AKA
SUCI
GUTI Refresh
After Registration
After Service Req.
Confidentiality Protection
NAS Signalling
RRC Signalling
User Data
Integrity Protection
NAS Signalling
RRC Signalling
User Data
UE Radio
Capabilities Tranfer
UE Network
Security Capabilities
Confidentiality Mechanisms
Supported by UE
Integrity Mechanisms
Supported by UE
Standard
Commercial
[16]
Operator A
Operator B
C
D
E
M A V C T B
M A V C T B
Beijing
5G SA Mandatory (TS 33.501 [3])
5G SA Optional (TS 33.501 [3])
5G Compliant
No 5G Compliant

Attacks in Actual 5G Commercial Networks

Subscriber Credentials

IMSI Catching



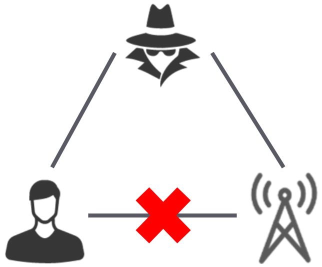
Tracking

No Confidentiality

Eavesdropping

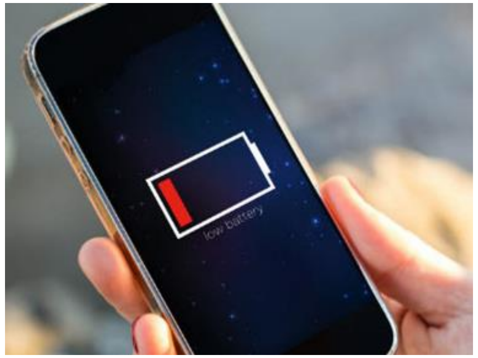
No Integrity

Manipulation



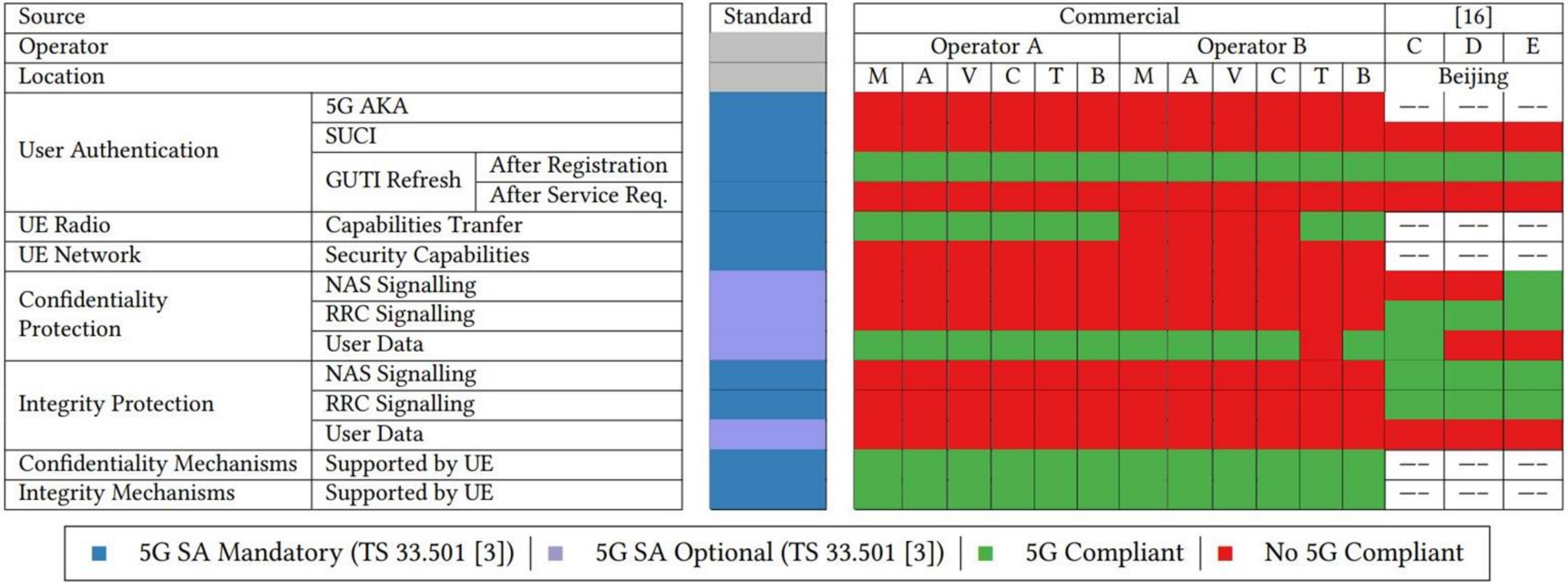
Authentication

Activity Monitoring



5G Security in the Wild

Security evaluation of commercial European mobile networks, unmasking supported 5G SA security features



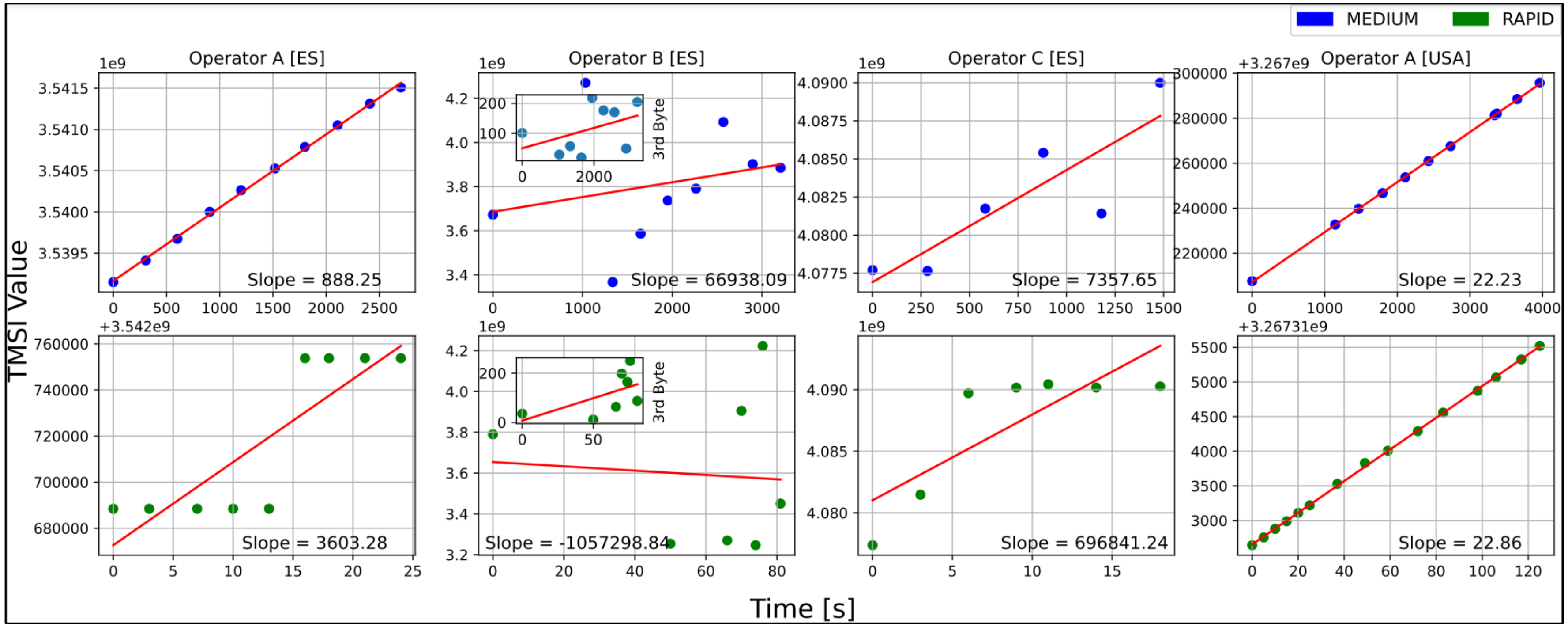
5G Security in the Wild

Country			Spain			France	United States				Beijing		
Operator			A	B		A	A		B	C	A	B	C
Deployment type: SA vs. NSA			NSA	NSA		NSA	SA	NSA	NSA	NSA	SA	SA	SA
Subscriber Identifiers	Ciphering of Permanent Identifiers												
	GUTI Refresh	After Registration											
		Periodic Registration									—	—	—
		After Service Request (Paging)											
Authentication Procedure	5G AKA										—	—	—
Control Plane Data (CP)	Confidentiality	NAS	EEA2	EEA2/1	EEA2/1	EEA2	NEA2	EEA2	EEA2	EEA3			
		RRC	EEA2	EEA2/1	EEA2/1	EEA2	NEA2	EEA1	EEA2	EEA2			
	Integrity	NAS	EIA2	EIA2	EIA2	EIA2	NIA2	EIA2	EIA2	EIA3			
		RRC	EIA2	EIA2	EIA2	EIA2	NIA2	EIA2	EIA2	EIA2			
User Plane Data (UP)	Confidentiality		NEA2	NEA2	NEA2	NEA2	NEA2	NEA2	NEA2	NEA2			
	Integrity						NIA2		NIA2				
Initial NAS message	Protection												
UE Radio Capabilities Transmission after RRC SMC											—	—	—

5G Compliant | 4G Compliant | No Security

Comparison between 5G SA and NSA implemented security features.

5G Security in the Wild



Evaluating the behaviour of temporary identifiers over time.

- Identifiers change not following proper randomization, leading to some traceable patterns
- Different mobile network carriers showed similar patterns

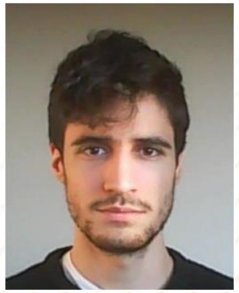
i2cat

5G and O-RAN Security Review Towards 6G

Security and Privacy attacks on Cellular Networks

Part 1: From 4G to 5G Systems Security

Practice



Óscar Lasierra

Pau Baguer

5G SA NAS Messages

SUPI Concealment

- Ciphering Subscriber Permanent Identifiers

5G Authentication

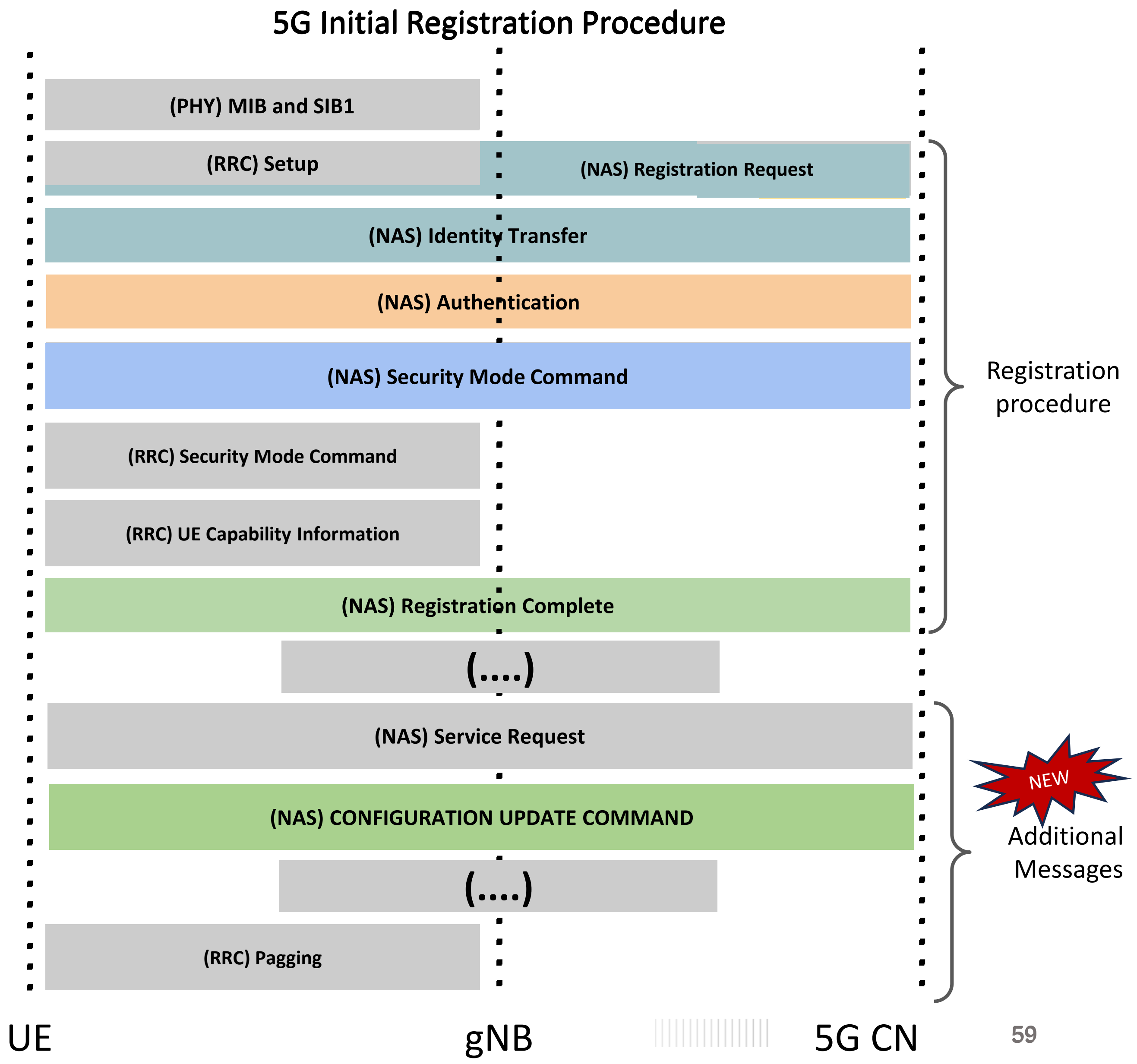
- AKA using new 5G Core Network Functions

5G-GUTI Refresh

- Refresh temporary identifiers after Registration Procedure and Service Request

NAS Integrity and Confidentiality

- Protect the initial NAS message
- UE integrity and confidentiality supported algorithms



5G SA NAS Messages

Files:

- 24May23_5gsa_bcn_NAS_short.txt

NAS Registration Request

```
Time:    18:44:29.904

REGISTRATION REQUEST        3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.6)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 41)
    Message number: 65
M 5GS registration type (hex data: 9)
    5GS registration type value: initial registration
    FOR: Follow-on request pending
M ngKSI (hex data: 0)
    TSC: native security context
    NAS key set identifier: 0
M 5GS mobile identity (hex data: 000bf212 f4308000 d8d20e8f 82)
    Type of identity: 5G-GUTI
    MCC: 214
    MNC: 3
    AMF Region ID: 128
    AMF Set ID: 3
    AMF Pointer: 24
    5G-TMSI: 0xd20e8f82
```

```
O UE security capability (hex data: 2e04f070 f070)
    5G-EA0: supported
    128-5G-EA1: supported
    128-5G-EA2: supported
    128-5G-EA3: supported
    5G-EA4: not supported
    5G-EA5: not supported
    5G-EA6: not supported
    5G-EA7: not supported
    5G-IA0: not supported
    128-5G-IA1: supported
    128-5G-IA2: supported
    128-5G-IA3: supported
    5G-IA4: not supported
    5G-IA5: not supported
    5G-IA6: not supported
    5G-IA7: not supported
    EEA0: supported
    128-EEA1: supported
    128-EEA2: supported
    128-EEA3: supported
    EEA4: not supported
    EEA5: not supported
    EEA6: not supported
    EEA7: not supported
    EIA0: not supported
    128-EIA1: supported
    128-EIA2: supported
    128-EIA3: supported
    EIA4: not supported
    EIA5: not supported
    EIA6: not supported
    EIA7: not supported
O NAS message container (hex data: 71003b51 0581ca9d c0010a3e 741c2aab db46c296 0cb
```

(NAS) Registration Request	(NAS) Identity Transfer	(NAS) Authentication	(NAS) Security Mode Command	(NAS) Registration Complete	(NAS) Configuration Update Command

NAS Registration Request

```
Time:    18:44:29.904

REGISTRATION REQUEST        3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.6)

M Extended protocol discriminator (hex data: 7e)
|    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
|    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 41)
|    Message number: 65
M 5GS registration type (hex data: 9)
|    5GS registration type value: initial registration
|    FOR: Follow-on request pending
M ngKSI (hex data: 0)
|    TSC: native security context
|    NAS key set identifier: 0
M 5GS mobile identity (hex data: 000bf212 f4308000 d8d20e8f 82)
|    Type of identity: 5G-GUTI
|    MCC: 214
|    MNC: 3
|    AMF Region ID: 128
|    AMF Set ID: 3
|    AMF Pointer: 24
|    5G-TMSI: 0xd20e8f82
```

```
O UE security capability (hex data: 2e04f070 f070)
|    5G-EA0: supported
|    128-5G-EA1: supported
|    128-5G-EA2: supported
|    128-5G-EA3: supported
|    5G-EA4: not supported
|    5G-EA5: not supported
|    5G-EA6: not supported
|    5G-EA7: not supported
|    5G-IA0: not supported
|    128-5G-IA1: supported
|    128-5G-IA2: supported
|    128-5G-IA3: supported
|    5G-IA4: not supported
|    5G-IA5: not supported
|    5G-IA6: not supported
|    5G-IA7: not supported
|    EEA0: supported
|    128-EEA1: supported
|    128-EEA2: supported
|    128-EEA3: supported
|    EEA4: not supported
|    EEA5: not supported
|    EEA6: not supported
|    EEA7: not supported
|    EIA0: not supported
|    128-EIA1: supported
|    128-EIA2: supported
|    128-EIA3: supported
|    EIA4: not supported
|    EIA5: not supported
|    EIA6: not supported
|    EIA7: not supported
O NAS message container (hex data: 71003b51 0581ca9d c0010a3e 741c2aab db46c296 0cb
```

NAS Identity Response

```
Time:    18:44:29.963

IDENTITY REQUEST        3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.21)

M Extended protocol discriminator (hex data: 7e)
|    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
|    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 5b)
|    Message number: 91
M Identity type (hex data: 1)
|    Type of identity: SUCI
M Spare Half Octet (hex data: 0)
```

```
Time:    18:44:29.963

IDENTITY RESPONSE       3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.22)

M Extended protocol discriminator (hex data: 7e)
|    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
|    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 5c)
|    Message number: 92
M Mobile identity (hex data: 000d0112 f430f0ff 00005628 844903)
|    Type of identity: SUCI
|    SUPI format: IMSI
|    MCC: 214
|    MNC: 3
|    Routing indicator digits: 0
|    Protection scheme identifier: Null scheme
|    Home network PKI: 0
|    MSIN: 6582489430
```

NAS Identity Response

```
Time:    18:44:29.963

IDENTITY REQUEST        3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.21)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 5b)
    Message number: 91
M Identity type (hex data: 1)
    Type of identity: SUCI
M Spare Half Octet (hex data: 0)
```

```
Time:    18:44:29.963

IDENTITY RESPONSE       3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.22)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 5c)
    Message number: 92
M Mobile identity (hex data: 000d0112 f430f0ff 00005628 844903)
    Type of identity: SUCI
    SUPI format: IMSI
    MCC: 214
    MNC: 3
    Routing indicator digits: 0
    Protection scheme identifier: Null scheme
    Home network PKI: 0
    MSIN: 6582489430
```

NAS Authentication

```
Time:    18:44:30.136

AUTHENTICATION REQUEST      3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.1)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 56)
    Message number: 86
M ngKSI (hex data: 1)
    TSC: native security context
    NAS key set identifier: 1
    RAAI: all PLMN registration area allocated
M Spare Half Octet (hex data: 0)
M ABBA (hex data: 020000)
O Authentication parameter RAND (hex data: 218aec5a 7d1df8e0 0ada6aa3 28ce1ecc 60)
    Authentication parameter RAND (hex):  8aec 5a7d 1df8 e00a da6a a328 ce1e cc60
O Authentication parameter AUTN  (hex data: 20108e9c 766a686b 8000b7d6 5f8c65c1 33ad)
    Authentication parameter AUTN (hex):  8e9c 766a 686b 8000 b7d6 5f8c 65c1 33ad
```

```
Time:    18:44:30.221

AUTHENTICATION RESPONSE     3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.2)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 57)
    Message number: 87
O Authentication parameter RAND (hex data: 2d10ac22 74590a6c 7b7d0ce8 469f5102 b164)
    RES: 0xac2274590a6c7b7d0ce8469f5102b164
```

NAS Authentication

```
Time:   18:44:30.136

AUTHENTICATION REQUEST     3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.1)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 56)
    Message number: 86
M ngKSI (hex data: 1)
    TSC: native security context
    NAS key set identifier: 1
    RAAI: all PLMN registration area allocated
M Spare Half Octet (hex data: 0)
M ABBA (hex data: 020000)
O Authentication parameter RAND (hex data: 218aec5a 7d1df8e0 0ada6aa3 28ce1ecc 60)
    Authentication parameter RAND (hex):  8aec 5a7d 1df8 e00a da6a a328 ce1e cc60
O Authentication parameter AUTN  (hex data: 20108e9c 766a686b 8000b7d6 5f8c65c1 33ad)
    Authentication parameter AUTN (hex):  8e9c 766a 686b 8000 b7d6 5f8c 65c1 33ad
```

```
Time:   18:44:30.221

AUTHENTICATION RESPONSE     3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.2)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 57)
    Message number: 87
O Authentication parameter RAND (hex data: 2d10ac22 74590a6c 7b7d0ce8 469f5102 b164)
    RES: 0xac2274590a6c7b7d0ce8469f5102b164
```

NAS Security Mode Command

```
Time:   18:44:30.260

SECURITY MODE COMMAND       3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.25)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 5d)
    Message number: 93
M Selected NAS security algorithms (hex data: 22)
    Integrity protection algorithm: 128-5G-IA2
    Ciphering algorithm: 128-5G-EA2
M ngKSI (hex data: 1)
    TSC: native security context
    NAS key set identifier: 1
    RAAI: all PLMN registration area allocated
M Spare Half Octet (hex data: 0)
M Replayed UE security capabilities (hex data: 04f070f0 70)
    5G-EA0: supported
    128-5G-EA1: supported
    128-5G-EA2: supported
    128-5G-EA3: supported
    5G-EA4: not supported
    5G-EA5: not supported
    5G-EA6: not supported
```

```
    EIA7: not supported
O IMEISV Request (hex data: e1)
    IMEISV request value: IMEISV requested
O Selected EPS NAS security algorithms (hex data: 5722)
    Type of integrity protection algorithm: EPS integrity algorithm 128-EIA2
    Type of ciphering algorithm: EPS encryption algorithm 128-EEA2
O Additional 5G security information (hex data: 360102)
    HDP: KAMF derivation is not required
    RINMR: Retransmission of the initial NAS message requested
O Replayed S1 UE security capabilities (hex data: 1904f070 c040)
    EPS encryption algorithms supported
        EEA0: supported
        128-EEA1: supported
        128-EEA2: supported
        128-EEA3: supported
        EEA4: not supported
        EEA5: not supported
        EEA6: not supported
        EEA7: not supported
    EPS integrity algorithms supported
        EIA0: not supported
        128-EIA1: supported
        128-EIA2: supported
        128-EIA3: supported
```

NAS Security Mode Command

```
Time:   18:44:30.260

SECURITY MODE COMMAND       3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.25)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 5d)
    Message number: 93
M Selected NAS security algorithms (hex data: 22)
    Integrity protection algorithm: 128-5G-IA2
    Ciphering algorithm: 128-5G-EA2
M ngKSI (hex data: 1)
    TSC: native security context
    NAS key set identifier: 1
    RAAI: all PLMN registration area allocated
M Spare Half Octet (hex data: 0)
M Replayed UE security capabilities (hex data: 04f070f0 70)
    5G-EA0: supported
    128-5G-EA1: supported
    128-5G-EA2: supported
    128-5G-EA3: supported
    5G-EA4: not supported
    5G-EA5: not supported
    5G-EA6: not supported
```

```
    EIA7: not supported
O IMEISV Request (hex data: e1)
    IMEISV request value: IMEISV requested
O Selected EPS NAS security algorithms (hex data: 5722)
    Type of integrity protection algorithm: EPS integrity algorithm 128-EIA2
    Type of ciphering algorithm: EPS encryption algorithm 128-EEA2
O Additional 5G security information (hex data: 360102)
    HDP: KAMF derivation is not required
    RINMR: Retransmission of the initial NAS message requested
O Replayed S1 UE security capabilities (hex data: 1904f070 c040)
    EPS encryption algorithms supported
        EEA0: supported
        128-EEA1: supported
        128-EEA2: supported
        128-EEA3: supported
        EEA4: not supported
        EEA5: not supported
        EEA6: not supported
        EEA7: not supported
    EPS integrity algorithms supported
        EIA0: not supported
        128-EIA1: supported
        128-EIA2: supported
```

NAS Security Mode Command

```
Time:    18:44:30.260

SECURITY MODE COMPLETE      3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.26)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 5e)
    Message number: 94
O IMEISV (hex data: 77000935 65549988 918313f2)
    Type of identity: IMEISV
    Identity digits: 3564599881938312
O NAS message container (hex data: 71003b7e 00410900 0bf212f4 308000d8 d20e8f82 10010
    Registration request
    Extended protocol discriminator (hex data: 7e)
        EPD value: 126 (5GS mobility management)
    Security header type (hex data: 0)
        Security header type: 0 (Plain 5GS NAS message, not security protected)
    Spare Half Octet (hex data: 0)
    Message Type (hex data: 41)
        Message number: 65
    5GS registration type (hex data: 9)
        5GS registration type value: initial registration
        FOR: Follow-on request pending
    ngKSI (hex data: 0)
        TSC: native security context
        NAS key set identifier: 0
```

```
5GS mobile identity (hex data: 000bf212 f4308000 d8d20e8f 82)
    Type of identity: 5G-GUTI
    MCC: 214
    MNC: 3
    AMF Region ID: 128
    AMF Set ID: 3
    AMF Pointer: 24
    5G-TMSI: 0xd20e8f82
5GMM capability (hex data: 100103)
    S1 mode: supported
    HO attach: supported
    LPP: not supported
    RestrictEC: not supported
    5G-CP CIoT: not supported
    N3 data: not supported
    5G-IPHC-CP CIoT: not supported
    SGC: not supported
UE security capability (hex data: 2e04f070 f070)
    5G-EA0: supported
    128-5G-EA1: supported
    128-5G-EA2: supported
    128-5G-EA3: supported
    5G-EA4: not supported
    5G-EA5: not supported
    5G-EA6: not supported
    5G-EA7: not supported
```

NAS Security Mode Command

```
Time:   18:44:30.260

SECURITY MODE COMPLETE      3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.26)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 5e)
    Message number: 94
O IMEISV (hex data: 77000935 65549988 918313f2)
    Type of identity: IMEISV
    Identity digits: 35645998881938312
O NAS message container (hex data: 71003b7e 00410900 0bf212f4 308000d8 d20e8f82 10010
    Registration request
    Extended protocol discriminator (hex data: 7e)
        EPD value: 126 (5GS mobility management)
    Security header type (hex data: 0)
        Security header type: 0 (Plain 5GS NAS message, not security protected)
    Spare Half Octet (hex data: 0)
    Message Type (hex data: 41)
        Message number: 65
    5GS registration type (hex data: 9)
        5GS registration type value: initial registration
        FOR: Follow-on request pending
    ngKSI (hex data: 0)
        TSC: native security context
        NAS key set identifier: 0
```

```
5GS mobile identity (hex data: 000bf212 f4308000 d8d20e8f 82)
    Type of identity: 5G-GUTI
    MCC: 214
    MNC: 3
    AMF Region ID: 128
    AMF Set ID: 3
    AMF Pointer: 24
    5G-TMSI: 0xd20e8f82
5GMM capability (hex data: 100103)
    S1 mode: supported
    HO attach: supported
    LPP: not supported
    RestrictEC: not supported
    5G-CP CIoT: not supported
    N3 data: not supported
    5G-IPHC-CP CIoT: not supported
    SGC: not supported
UE security capability (hex data: 2e04f070 f070)
    5G-EA0: supported
    128-5G-EA1: supported
    128-5G-EA2: supported
    128-5G-EA3: supported
    5G-EA4: not supported
    5G-EA5: not supported
    5G-EA6: not supported
    5G-EA7: not supported
```

NAS Registration Accept and Complete

```
Time:   18:44:30.565

REGISTRATION ACCEPT     3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.7)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protect
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 42)
    Message number: 66
M 5GS registration result (hex data: 0109)
    5GS registration result value: 3GPP access
    SMS allowed: SMS over NAS allowed
    NSSAA Performed: is not to be performed
    Emergency registered: Not registered for emergency services
O 5G-GUTI (hex data: 77000bf2 12f43080 00d8d20f 8f83)
    Type of identity: 5G-GUTI
    MCC: 214
    MNC: 3
    AMF Region ID: 128
    AMF Set ID: 3
    AMF Pointer: 24
    5G-TMSI: 0xd20f8f83
O TAI list (hex data: 54070012 f4300008 b6)
    Partial tracking area identity list 1
        Type of list: TACs belonging to one PLMN, with non-consecutive TAC values
        Number of elements: 1
        MCC: 214
        MNC: 3
        TAC: 2230 (0x0008B6)
O Allowed NSSAI (hex data: 15050401 000001)
```

```
O Allowed NSSAI (hex data: 15050401 000001)
    S-NSSAI value 1
        SST: 1
        SD: 1
O 5GS network feature support (hex data: 210191)
    IMS VoPS: supported over 3GPP access
    EMC: not supported
    EMF: not supported
    IWKN26: Interworking without N26 not supported
    MPSI: Access identity 1 valid in RPLMN or equivalent PLMN
O PDU session status (hex data: 50020000)
    PSI(1) - PSI(15): all PDU SESSION INACTIVE
O T3512 value (hex data: 5e0105)
    Unit: value is incremented in multiples of 10 minutes
    Timer value: 5
O T3502 value (hex data: 16012c)
    Unit: value is incremented in multiples of 1 minute
    Timer value: 12
O Emergency Number List (hex data: 3404031f 11f2)
    Emergency Service Category Value: 0x1f (Police,Ambulance,Fire Brigade,Marine Guard,Mountain Rescue)
    Emergency Number: 112
O NSSAI inclusion mode (hex data: a3)
    NSSAI inclusion mode: D
```

NAS Registration Accept and Complete

```
Time:   18:44:30.565

REGISTRATION ACCEPT     3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.7)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protect
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 42)
    Message number: 66
M 5GS registration result (hex data: 0109)
    5GS registration result value: 3GPP access
    SMS allowed: SMS over NAS allowed
    NSSAA Performed: is not to be performed
    Emergency registered: Not registered for emergency services
O 5G-GUTI (hex data: 77000bf2 12f43080 00d8d20f 8f83)
    Type of identity: 5G-GUTI
    MCC: 214
    MNC: 3
    AMF Region ID: 128
    AMF Set ID: 3
    AMF Pointer: 24
    5G-TMSI: 0xd20f8f83
O TAI list (hex data: 54070012 f4300008 b6)
    Partial tracking area identity list 1
        Type of list: TACs belonging to one PLMN, with non-consecutive TAC values
        Number of elements: 1
        MCC: 214
        MNC: 3
        TAC: 2230 (0x0008B6)
O Allowed NSSAI (hex data: 15050401 000001)
```

```
O Allowed NSSAI (hex data: 15050401 000001)
    S-NSSAI value 1
        SST: 1
        SD: 1
O 5GS network feature support (hex data: 210191)
    IMS VoPS: supported over 3GPP access
    EMC: not supported
    EMF: not supported
    IWKN26: Interworking without N26 not supported
    MPSI: Access identity 1 valid in RPLMN or equivalent PLMN
O PDU session status (hex data: 50020000)
    PSI(1) - PSI(15): all PDU SESSION INACTIVE
O T3512 value (hex data: 5e0105)
    Unit: value is incremented in multiples of 10 minutes
    Timer value: 5
O T3502 value (hex data: 16012c)
    Unit: value is incremented in multiples of 1 minute
    Timer value: 12
O Emergency Number List (hex data: 3404031f 11f2)
    Emergency Service Category Value: 0x1f (Police,Ambulance,Fire Brigade,Marine Guard,Mountain Rescue)
    Emergency Number: 112
O NSSAI inclusion mode (hex data: a3)
    NSSAI inclusion mode: D
```

Additional Messages - Configuration Update Command after Service Request

```
Time:    18:48:32.859

SERVICE REQUEST     3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.16)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security pro
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 4c)
    Message number: 76
M ngKSI (hex data: 1)
    TSC: native security context
    NAS key set identifier: 1
M Service type (hex data: 2)
    Service type: mobile terminated services
M 5G-S-TMSI (hex data: 0007f400 d8d20f8f 83)
    Type of identity: 5G-S-TMSI
    AMF Set ID: 3
    AMF Pointer: 24
    5G-TMSI: 0xd20f8f83
O NAS message container (hex data: 710011e3 c3e0eb3f 19dbafd7 997ab3
```

```
Time:    18:48:33.125

CONFIGURATION UPDATE COMMAND       3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.19)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 54)
    Message number: 84
O Configuration update indication (hex data: d1)
    ACK: acknowledgement requested
    RED: registration not requested
O 5G-GUTI (hex data: 77000bf2 12f43080 00d8d210 8f3f)
    Type of identity: 5G-GUTI
    MCC: 214
    MNC: 3
    AMF Region ID: 128
    AMF Set ID: 3
    AMF Pointer: 24
    5G-TMSI: 0xd2108f3f
```

Additional Messages - Configuration Update Command after Service Request

```
Time:   18:48:32.859

SERVICE REQUEST    3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.16)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security pro
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 4c)
    Message number: 76
M ngKSI (hex data: 1)
    TSC: native security context
    NAS key set identifier: 1
M Service type (hex data: 2)
    Service type: mobile terminated services
M 5G-S-TMSI (hex data: 0007f400 d8d20f8f 83)
    Type of identity: 5G-S-TMSI
    AMF Set ID: 3
    AMF Pointer: 24
    5G-TMSI: 0xd20f8f83
O NAS message container (hex data: 710011e3 c3e0eb3f 19dbafd7 997ab3
```

```
Time:   18:48:33.125

CONFIGURATION UPDATE COMMAND      3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.19)

M Extended protocol discriminator (hex data: 7e)
    EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
    Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 54)
    Message number: 84
O Configuration update indication (hex data: d1)
    ACK: acknowledgement requested
    RED: registration not requested
O 5G-GUTI (hex data: 77000bf2 12f43080 00d8d210 8f3f)
    Type of identity: 5G-GUTI
    MCC: 214
    MNC: 3
    AMF Region ID: 128
    AMF Set ID: 3
    AMF Pointer: 24
    5G-TMSI: 0xd2108f3f
```

(NAS) Registration Request	(NAS) Identity Transfer	(NAS) Authentication	(NAS) Security Mode Command	(NAS) Registration Complete	(NAS) Configuration Update Command

TMSI Referesh (one UE/User)

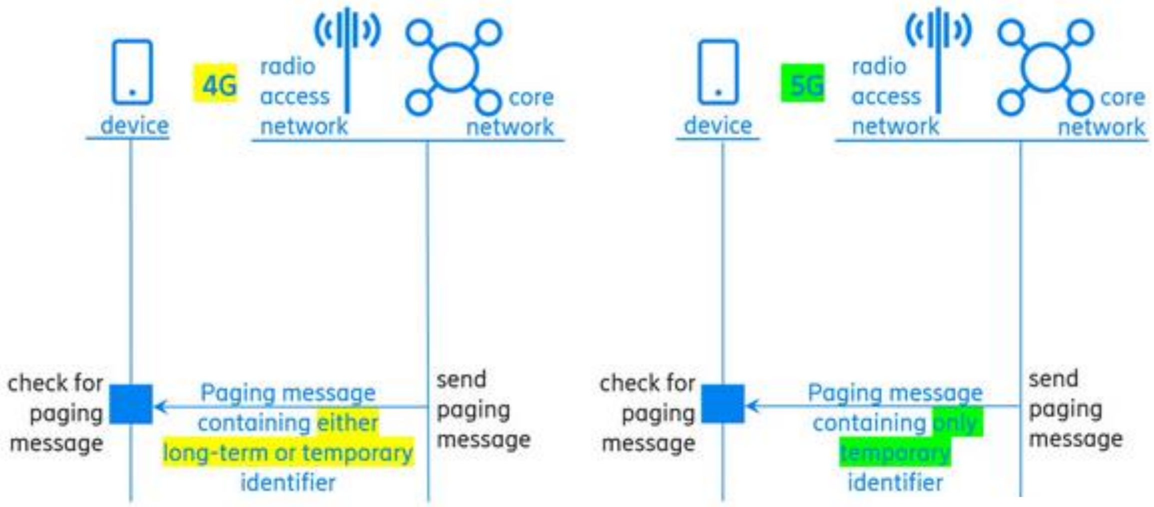
Time	Technology	Message	MME/AMF Group/Set ID	MME/AMF Code/Pointer	M_TMSI
18:44:29.904	5G_SA	REGISTRATION REQUEST	3	24	0xd20e8f82
18:44:30.565	5G_SA	REGISTRATION ACCEPT	3	24	0xd20f8f83
18:47:00.836	5G_SA	SERVICE REQUEST	3	24	0xd20f8f83
18:47:47.295	5G_SA	SERVICE REQUEST	3	24	0xd20f8f83
18:48:32.859	5G_SA	SERVICE REQUEST	3	24	0xd20f8f83
18:48:33.125	5G_SA	CONFIGURATION UPDATE COMMAND	3	24	0xd2108f3f
18:48:41.068	4G	TRACKING AREA UPDATE REQUEST	8000	d8	d2108f3f
18:48:41.840	4G	TRACKING AREA UPDATE ACCEPT	8000	50	fa8d8f93
18:49:30.813	4G	TRACKING AREA UPDATE REQUEST	8000	50	fa8d8f93
18:49:30.813	5G_SA	REGISTRATION REQUEST	1	16	0xfa8d8f93
18:49:31.795	5G_SA	REGISTRATION ACCEPT	3	24	0xd2108f9f
18:49:44.409	4G	TRACKING AREA UPDATE REQUEST	8000	d8	d2108f9f
18:49:45.121	4G	TRACKING AREA UPDATE ACCEPT	8000	50	fa8e8f30
18:49:47.371	4G	TRACKING AREA UPDATE REQUEST	8000	50	fa8e8f30
18:50:07.396	4G	TRACKING AREA UPDATE REQUEST	8000	50	fa8e8f30
18:50:07.396	5G_SA	REGISTRATION REQUEST	1	16	0xfa8e8f30
18:50:08.161	5G_SA	REGISTRATION ACCEPT	3	24	0xd2108fa9
18:50:10.517	5G_SA	SERVICE REQUEST	3	24	0xd2108fa9
18:50:10.607	5G_SA	CONFIGURATION UPDATE COMMAND	3	24	0xd2108faa
18:50:20.786	5G_SA	SERVICE REQUEST	3	24	0xd2108faa
18:51:01.722	5G_SA	SERVICE REQUEST	3	24	0xd2108faa
18:51:01.872	5G_SA	CONFIGURATION UPDATE COMMAND	3	24	0xd2108fbe
18:51:50.550	5G_SA	SERVICE REQUEST	3	24	0xd2108fbe
18:51:50.716	5G_SA	CONFIGURATION UPDATE COMMAND	3	24	0xd2118f17

(NAS) Registration Request	(NAS) Identity Transfer	(NAS) Authentication	(NAS) Security Mode Command	(NAS) Registration Complete	(NAS) Configuration Update Command

TMSI Referesh (one UE/User)

Time	Technology	Message	MME/AMF Group/Set ID	MME/AMF Code/Pointer	M_TMSI
18:44:29.904	5G_SA	REGISTRATION REQUEST	3	24	0xd20e8f82
18:44:30.565	5G_SA	REGISTRATION ACCEPT	3	24	0xd20f8f83
18:47:00.836	5G_SA	SERVICE REQUEST	3	24	0xd20f8f83
18:47:47.295	5G_SA	SERVICE REQUEST	3	24	0xd20f8f83
18:48:32.859	5G_SA	SERVICE REQUEST	3	24	0xd20f8f83
18:48:33.125	5G_SA	CONFIGURATION UPDATE COMMAND	3	24	0xd2108f3f
18:48:41.068	4G	TRACKING AREA UPDATE REQUEST	8000	d8	d2108f3f
18:48:41.840	4G	TRACKING AREA UPDATE ACCEPT	8000	50	fa8d8f93
18:49:30.813	4G	TRACKING AREA UPDATE REQUEST	8000	50	fa8d8f93
18:49:30.813	5G_SA	REGISTRATION REQUEST	1	16	0xfa8d8f93
18:49:31.795	5G_SA	REGISTRATION ACCEPT	3	24	0xd2108f9f
18:49:44.409	4G	TRACKING AREA UPDATE REQUEST	8000	d8	d2108f9f
18:49:45.121	4G	TRACKING AREA UPDATE ACCEPT	8000	50	fa8e8f30
18:49:47.371	4G	TRACKING AREA UPDATE REQUEST	8000	50	fa8e8f30
18:50:07.396	4G	TRACKING AREA UPDATE REQUEST	8000	50	fa8e8f30
18:50:07.396	5G_SA	REGISTRATION REQUEST	1	16	0xfa8e8f30
18:50:08.161	5G_SA	REGISTRATION ACCEPT	3	24	0xd2108fa9
18:50:10.517	5G_SA	SERVICE REQUEST	3	24	0xd2108fa9
18:50:10.607	5G_SA	CONFIGURATION UPDATE COMMAND	3	24	0xd2108faa
18:50:20.786	5G_SA	SERVICE REQUEST	3	24	0xd2108faa
18:51:01.722	5G_SA	SERVICE REQUEST	3	24	0xd2108faa
18:51:01.872	5G_SA	CONFIGURATION UPDATE COMMAND	3	24	0xd2108fbe
18:51:50.550	5G_SA	SERVICE REQUEST	3	24	0xd2108fbe
18:51:50.716	5G_SA	CONFIGURATION UPDATE COMMAND	3	24	0xd2118f17

Additional Messages - RRC Paging Message



While in 4G, the paging identifier could be either a long-term or a temporary identifier, on 5G networks, it can only be a temporary identifier. To illustrate how this can look, the paging identifiers are as shown below:

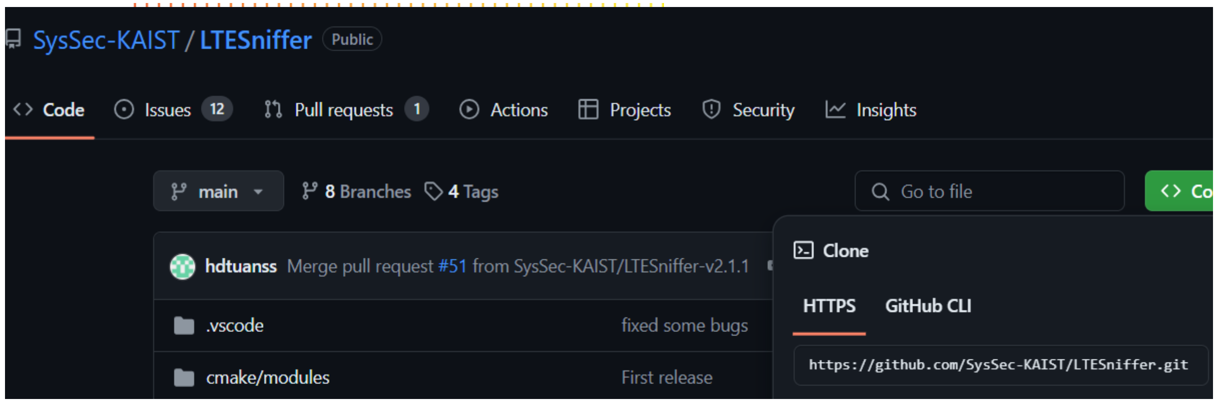
In 4G	In 5G
Paging identifier can be either: — long-term identifier, IMSI, — temporary identifier, S-TMSI.	Paging identifier can only be: — temporary identifier, 5G-S-TMSI or I-RNTI.

Additional Messages - RRC Paging Message

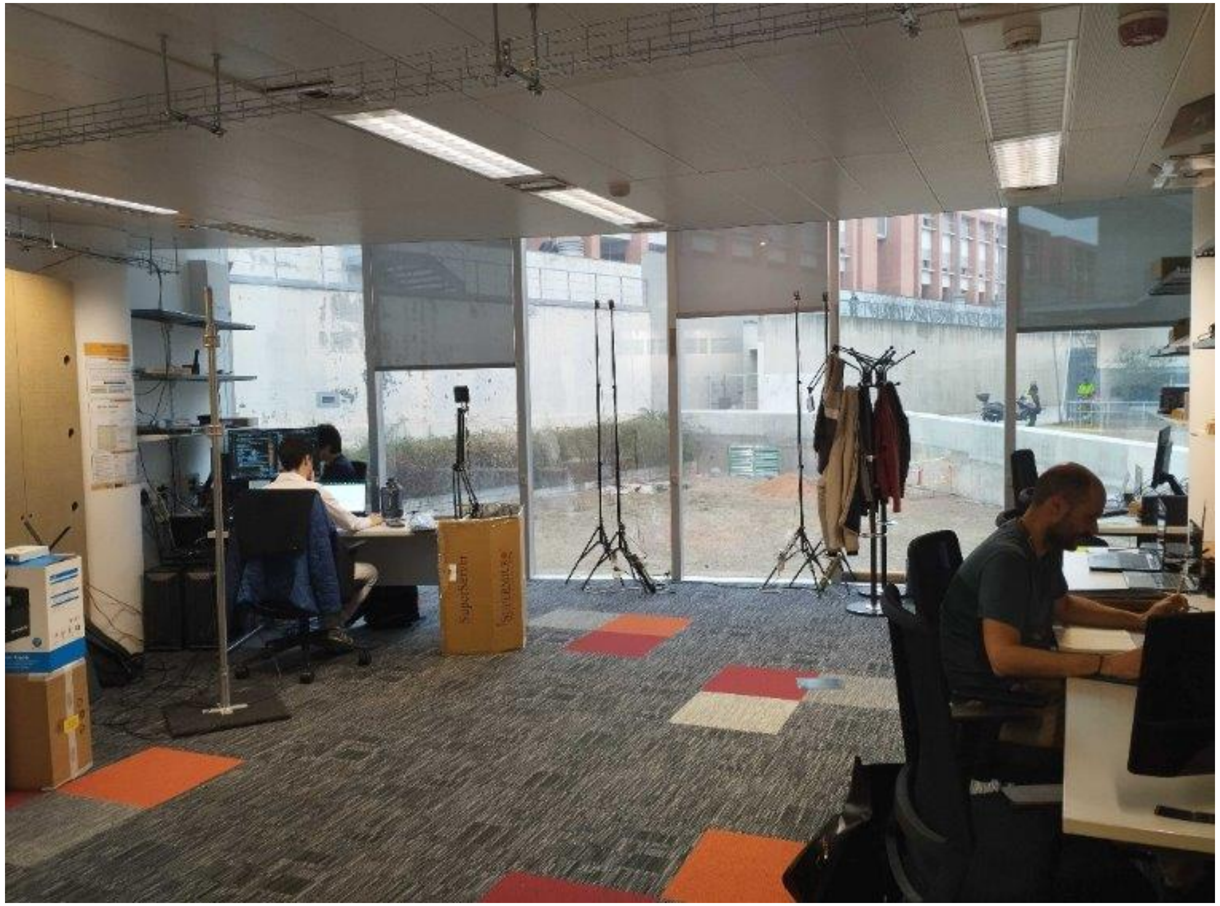
```
Time: 18:48:35.417

Paging  (3GPP TS 38.331 ver 16.6.0 Rel 16)

PCCH-Message
  message
    c1
      paging
        pagingRecordList
          pagingRecordList value 1
            ue-Identity
              ng-5G-S-TMSI
                Bin : '00D0EB4EFA06'H (48 bits)
```

```
Time: 18:48:41.957

Paging  (3GPP TS 36.331 ver 16.6.0 Rel 16)

PCCH-Message
  message
    c1
      paging
        pagingRecordList
          pagingRecordList value 1
            ue-Identity
              s-TMSI
                mmec
                  Bin : '58'H (= 88)
                m-TMSI
                  Bin : 'DE0411A3'H (32 bits)
            cn-Domain : ps
          pagingRecordList value 2
            ue-Identity
              s-TMSI
                mmec
                  Bin : '40'H (= 64)
                m-TMSI
                  Bin : 'DE1BB570'H (32 bits)
            cn-Domain : ps
```

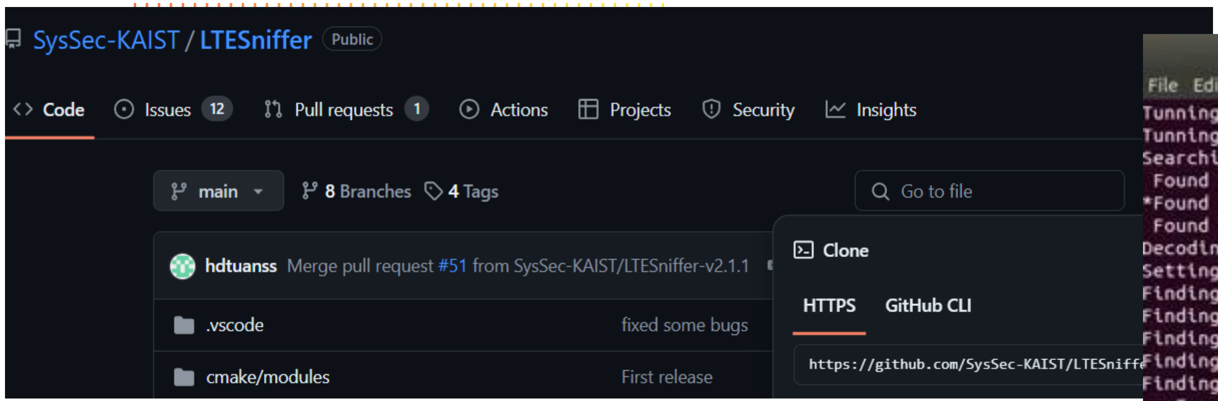
Additional Messages - RRC Paging Message - Exploiting 4G Paging Vulnerability

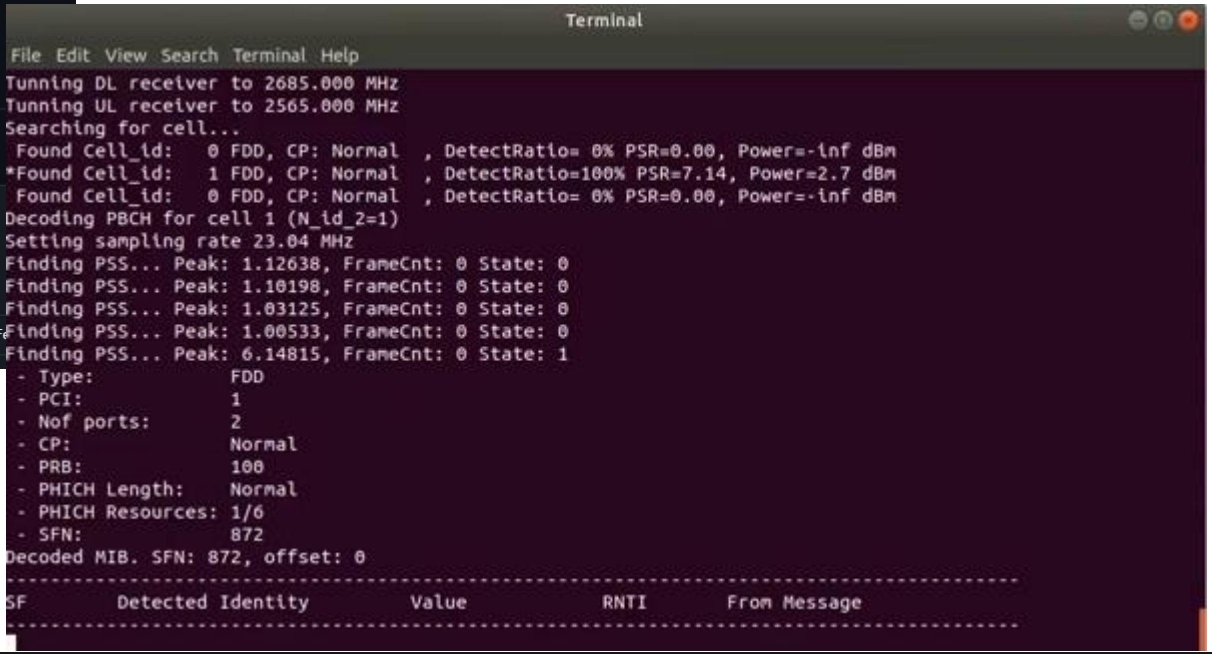


X310



Additional Messages - RRC Paging Message - Exploiting 4G Paging Vulnerability





{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:23:53 2024","tti":1459,"value":"214075546737905"}
{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:24:01 2024","tti":8819,"value":"214075546737905"}
{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:24:18 2024","tti":5939,"value":"214075546737905"}
{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:24:25 2024","tti":2739,"value":"214075546737905"}
{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:27:56 2024","tti":8799,"value":"214075541126127"}
{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:29:54 2024","tti":3489,"value":"214075544764540"}
{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:30:01 2024","tti":289,"value":"214075544764540"}
{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:31:56 2024","tti":2499,"value":"214075507683225"}
…. . . . .

RRC Paging Message - Exploiting 4G Paging Vulnerability – Exercice!

Files:

- Imsi.py
- identifiers_1.json

https://en.wikipedia.org/wiki/Mobile_country_code

Additional Messages - RRC Paging Message - Exploiting 4G Paging Vulnerability

{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:23:53 2024","tti":1459,"value":"214075546737905"}
{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:24:01 2024","tti":8819,"value":"214075546737905"}
{"id":3,"id_name":"IMSI","msg":5,"msg_name":"Paging","rnti":65534,"timestamp":"Tue May 21 16:24:18 2024","tti":5939,"value":"214075546737905"}
…........

Country and Operator User Counts (sorted from highest to lowest):

	MCC	MNC	user_count	Country	Operator
4	214	07	183	Spain	Movistar
11	232	03	11	Austria	T-Mobile
7	222	88	8	Italy	Wind Tre
16	262	03	4	Unknown	Unknown
3	214	05	4	Spain	Vodafone
0	204	08	3	Netherlands	KPN
5	214	22	3	Spain	Yoigo
14	260	01	3	Poland	Plus
12	234	10	2	UK	O2
15	262	01	2	Germany	Telekom
17	262	07	2	Germany	O2
18	268	03	2	Unknown	Unknown
20	310	17	2	Unknown	Unknown
10	228	03	1	Switzerland	Salt
9	228	02	1	Unknown	Unknown
1	206	20	1	Unknown	Unknown
2	208	20	1	France	Bouygues Telecom
8	222	99	1	Italy	3 Italia
6	222	01	1	Italy	TIM
13	234	20	1	UK	3
19	302	72	1	Unknown	Unknown
21	334	02	1	Mexico	Telcel
22	425	02	1	Unknown	Unknown
23	454	12	1	Hong Kong	CMHK
24	621	30	1	Nigeria	MTN Nigeria
25	722	07	1	Argentina	Movistar
26	730	02	1	Chile	Movistar

Repeated Users:

	IMSI	count
0	214075536230388	6
1	214075541849321	4
2	214075546737905	4
3	214075510387165	4
4	214075540203677	3
5	214075553343359	3
6	214075526245730	3
7	214075505508844	3
8	214075528085906	3
9	214050122675058	3
10	214075526386841	3
11	214075514595569	3
12	214075516572883	3
13	214075528012423	3
14	214075526710776	2
15	214075549072414	2
16	214075506437648	2
17	214075536773944	2
18	214075500397121	2
19	214075533029901	2
20	214075526376678	2
21	214075510389470	2
22	214075549928972	2
23	214075556410243	2
24	214075549811494	2
25	214075557103334	2
26	214075532565805	2

i2cat

5G and O-RAN Security Review Towards 6G

Security and Privacy attacks on Cellular Networks

Part 2: Open Radio Access Networks (O-RAN)

Theory

Esteban Municio

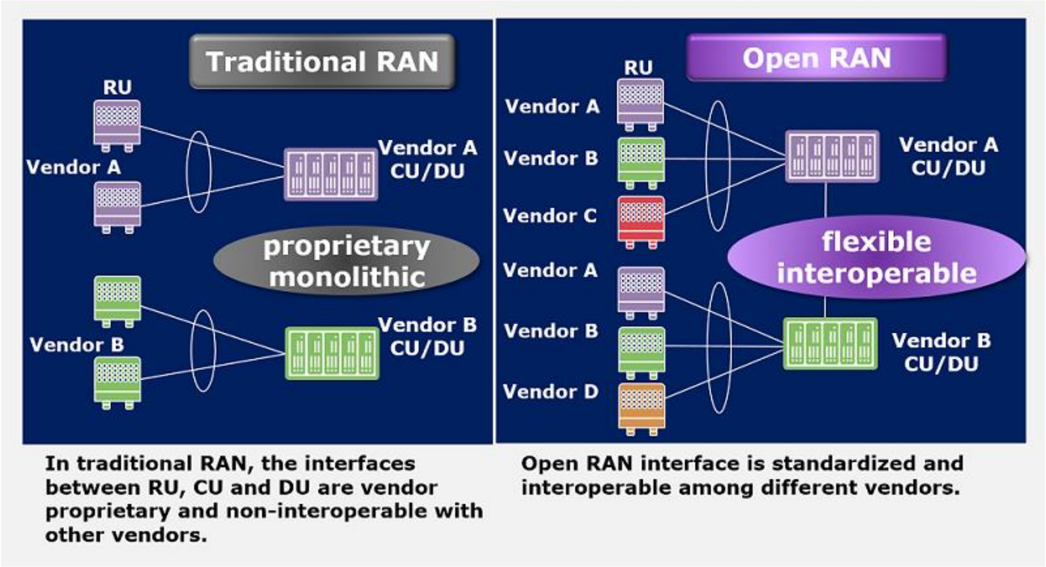
Ginés García

Xavier Costa

Open RAN

Open and virtualized RANs

- **Disaggregating** Radio Access Networks
  - Horizontal disaggregation of the network functions (RU/DU/CU) with open interfaces, defined as Open RAN
  - Vertical disaggregation of hardware and software with virtualization technologies, or vRAN



5G Hacking


IEEE Spectrum 5G Networks Are Worryingly Hackable

Type to search

NEWS TELECOMMUNICATIONS

5G Networks Are Worryingly Hackable › A shift to the cloud is opening the industry up to new attacks

BY EDD GENT | 24 AUG 2022 | 5 MIN READ

- Reported breaches of live 5G networks in “Red Teaming” exercises
  - Hackers hired by a company to test their defences
  - They were able to take control of the network potentially allowing them to disrupt operations

- The hacks were made possible thanks to *poorly configured **cloud** technology*

Open Radio Access Networks - Status

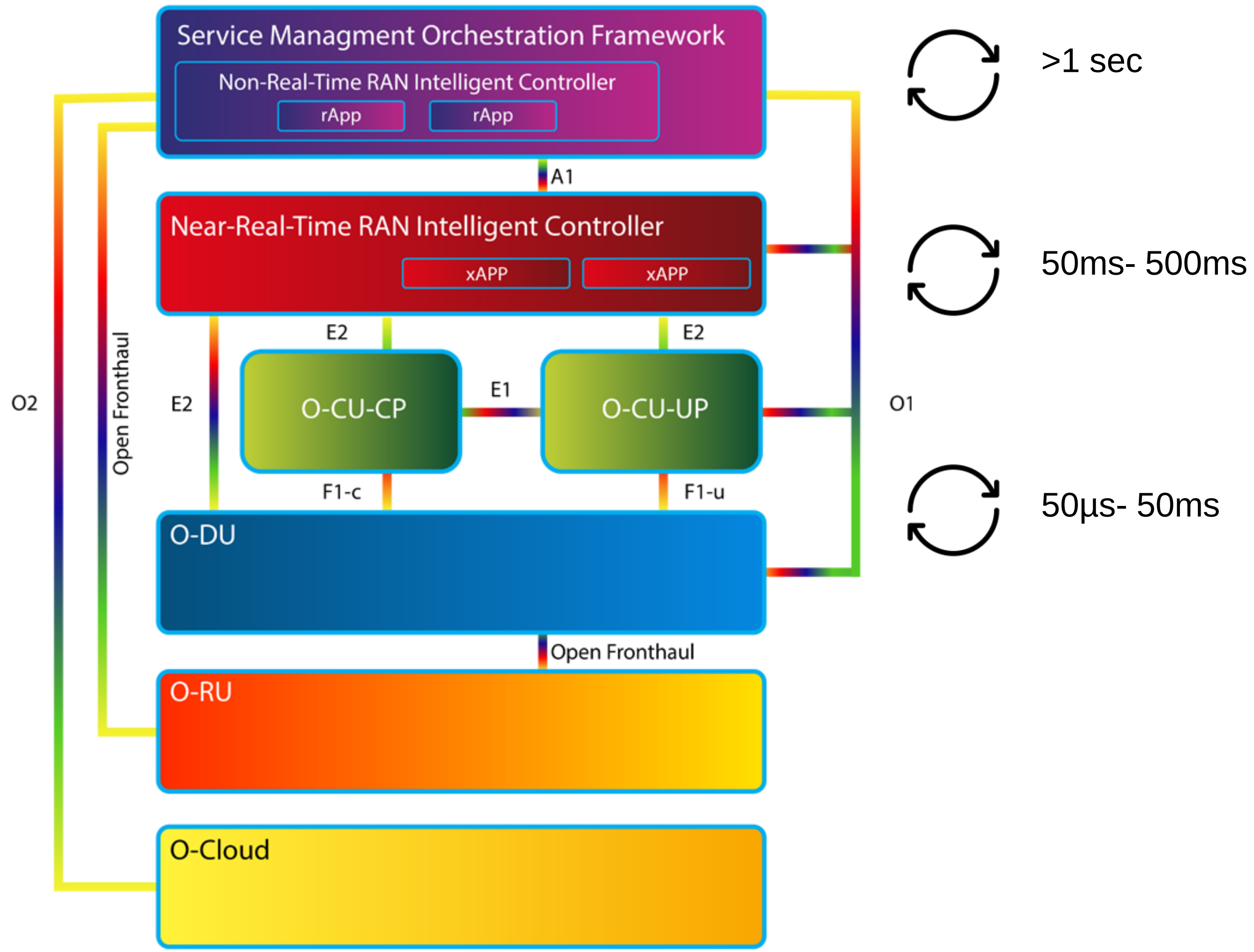
O-RAN Alliance

- **Carriers**
  - 24+ mobile operators across 4 continents
- **Membership**
  - 160+ companies
- **Technical Specs**
  - 40+ within 2 years
  - Aligned with SDOs
- **Open-source code**
  - 1.3+ million lines of code

Open RANs – What's New?

O-RAN Architecture

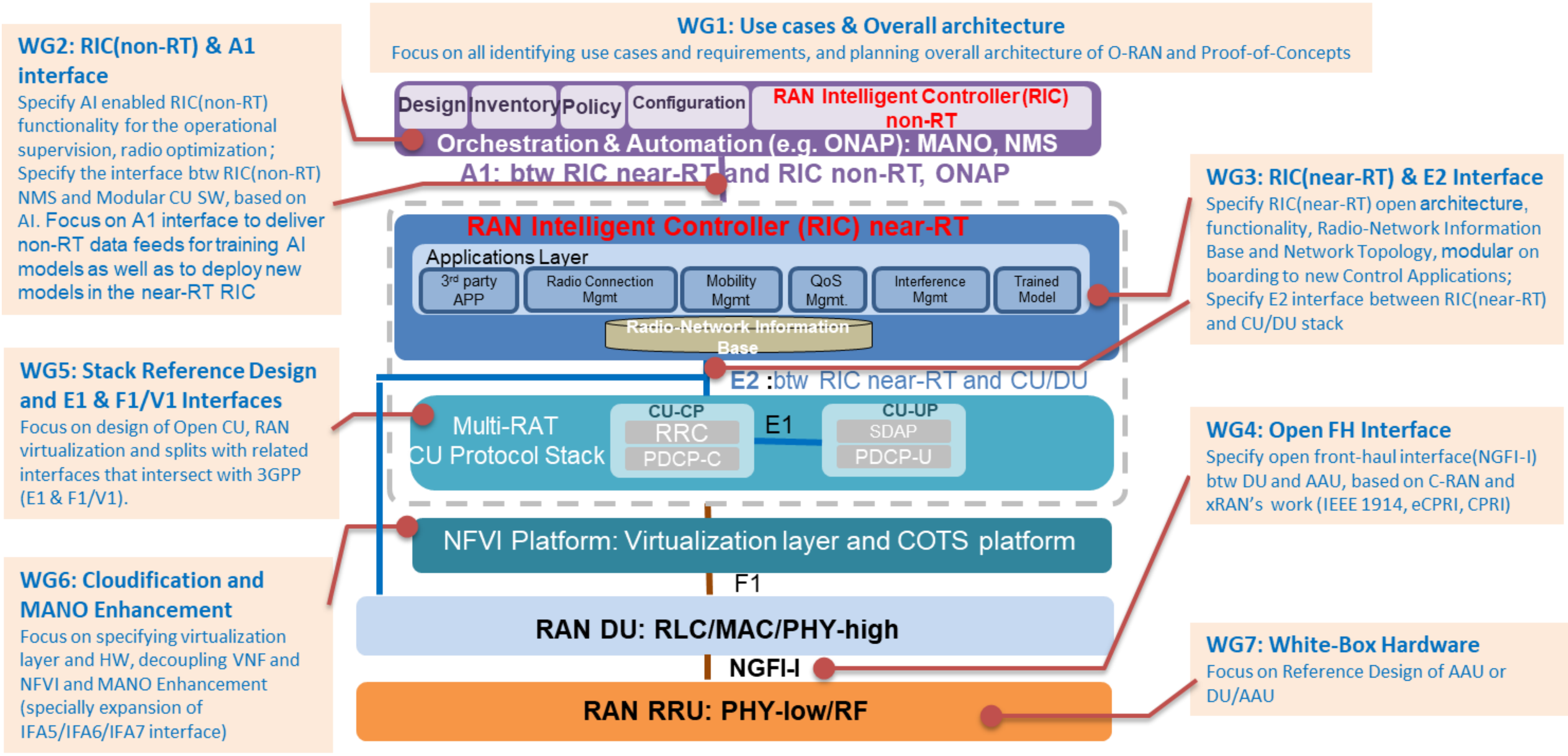
- Open Interfaces
  - Lower market entry barrier
    - *Increased RAN ecosystem*
    - *160+ companies*
  - Foster Innovation
    - *Smaller companies*
    - *Focusing on narrower topics*
- RAN Virtualization
  - O-Cloud
  - Acceleration Abstraction Layer (AAL)
- Automated Management and control
  - AI/ML native integration
  - xApps/rApps



Open RANs

O-RAN Architecture

- Open Interfaces
- Lower market entry barrier
- Foster Innovation
- RAN Virtualization
- Automated Management and control



Orchestrating a brighter world

Open Radio Access Networks – The Challenges

- **Market Share Forecasts**
  - Open RAN is expected to cover only about 10% of the overall market by 2025
- **Technical Issues**
  - **Increased complexity**
    - Interoperability
    - Optimization
    - Security

Ericsson issues warning on open RAN security

News Analysis
MIKE DANO, Editorial Director, 5G & Mobile Strategies
9/10/2020

Ericsson issued a broad warning Thursday to the wireless industry about the security of open RAN technology. The company listed a number of specific security issues that it said need to be addressed before the technology is widely deployed, and argued that "with any nascent technology, including O-RAN, security cannot be an afterthought and should be built upon a security-by-design approach."

The company's stance on the topic, complete with a 14-page white paper, is noteworthy considering the growing noise around the open RAN topic – as well as the effect the technology could have on Ericsson specifically and the wider telecom industry in general.

Open RAN promises to separate the various elements in a wireless network so that network operators can mix and match products from different vendors – a

Nokia halts O-RAN work on fear of US penalties for China links

News Analysis
IAIN MORRIS, International Editor
8/30/2021

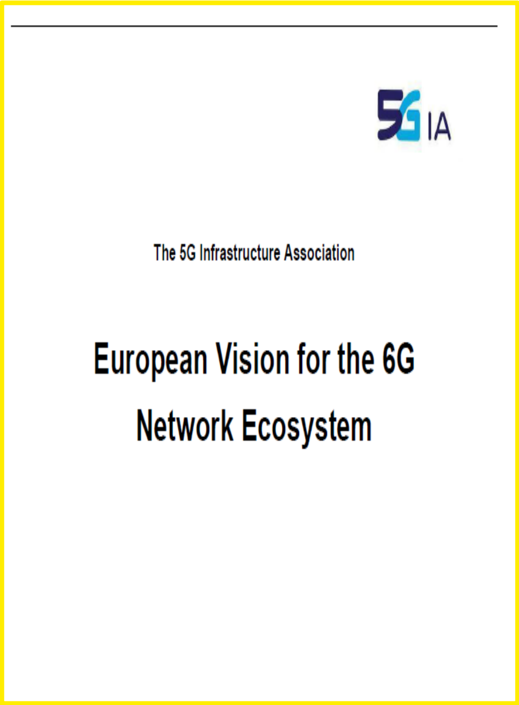
Mingling with Chinese companies named on the US naughty list has suddenly rattled Nokia.

The Finnish equipment maker has been a member of the O-RAN Alliance ever since its inception. It also claims to be one of the most active contributors to the group's work of developing more interoperable specifications for mobile networks. But all that has stopped – temporarily, at least.

Just weeks after another Chinese member was named on the Entity List – a trade blacklist maintained by the US government – Nokia is shutting down its O-RAN Alliance burners. Its fear seems to be that working alongside companies deemed criminals by the Biden administration could expose Nokia to US sanctions.

Dell'Oro Group, "Open RAN Market Expected to Approach $10 B, According to Dell'Oro Group," Online: https://www.delloro.com/news/open-ran-market-expected-to-approach-10-b/, Feb. 2021

EU 6G Vision White Paper


The 5G Infrastructure Association

European Vision for the 6G Network Ecosystem

- “3GPP and Open RAN concepts allow RAN equipment and software from different vendors to communicate and interoperate”

- “Multi-vendor decomposition and supply chain may *<u>increase the threat surface for malicious attacks</u>* as well as the operational complexity of the network.“

\Orchestrating a brighter world NEC

O-RAN Security

Technical workgroup (WG)		Focus area
WG 1	Use Cases and Overall Architecture	Identification of key O-RAN optimization and management use cases, deployment scenarios and overall architecture
WG 2	Non-RT RIC and A1 Interface	Optimization and automation of the RAN Radio Resource Management (RRM), higher layer procedure optimization using the RAN Intelligent Controller (RIC). Also providing AI/ML models to RAN functions
WG 3	Near-RT RIC and E2 Interface	
WG 4	Open Fronthaul Interfaces	Designing open interfaces to efficiently enable interoperability between different RAN hardware and software vendors
WG 5	Open F1/W1/E1/X2/Xn Interface	
WG 6	Cloudification and Orchestration	Commoditization, virtualization and modularization of multi-vendor RAN hardware and software
WG 7	White-box Hardware	
WG 8	Stack References Design	
WG 9	Open X-haul Transport	Designing new open transport network based on new architectures and end-user service requirements for fronthaul, mid-haul and backhaul
WG 10	OAM for O-RAN	Studying the O1 interface Operational and Management (OAM) specifications, and providing coordinated definition and collection of O1 key performance indicators (KPIs) across all WGs
WG 11	Security Work Group	Developing the security aspects of the open RAN ecosystem

O-RAN has established Working Group 11 (WG11) to ensure that the new specifications are secure by design

WG11 provides procedures to identify threats and assess and mitigate risks

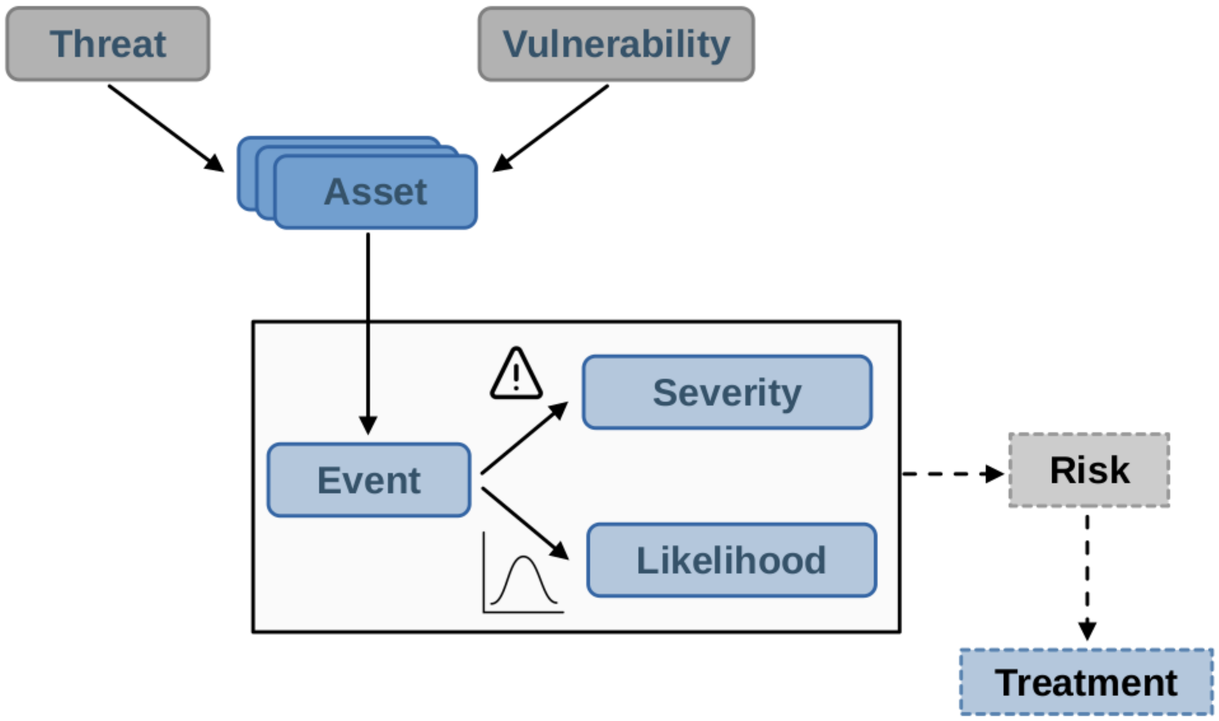
To date, 60% of those identified risks by WG11 are related to Denial-of-Service (DoS) and performance degradation

The use of open and cloud-based architectures increases the potential attack surface of RAN systems

i2cat
\Orchestrating a brighter world NEC

O-RAN Security: Analysis methodology

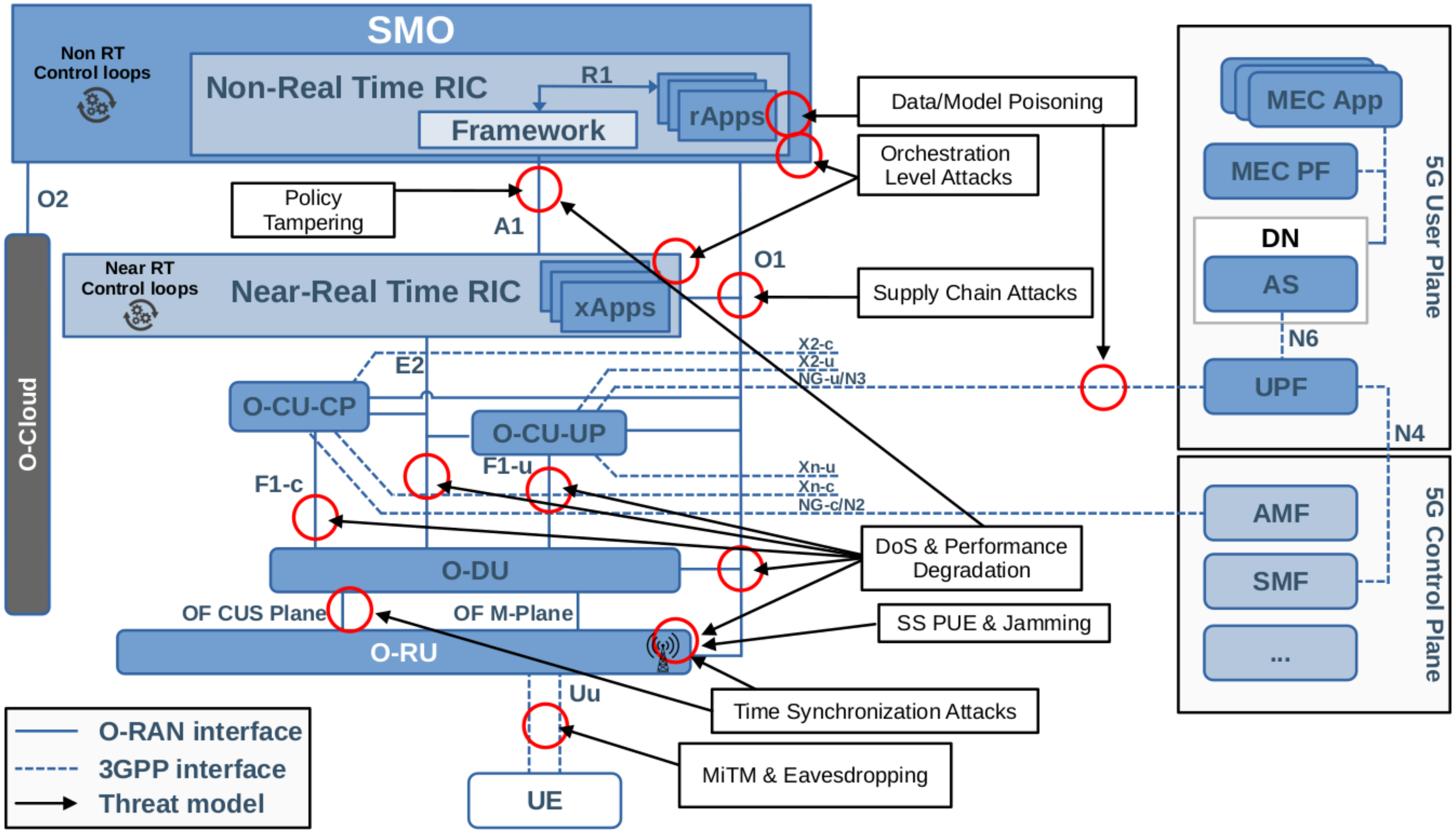
- New security challenges from the newly expended threat surface
- O-RAN WG11 threat model:
  - Risk Identification
  - Risk Assessment
  - Risk Mitigation



O-RAN Risk Identification

Threat:

"...any circumstance with the potential to adversely impact operations and assets, via unauthorized access, destruction, disclosure or modification of information, and denial of service"



Groups of threat surfaces:

- Functions, Interfaces, Architecture, Trust Chain, Virtualization, Open-source code

\Orchestrating a brighter world

O-RAN Risk Identification

Vulnerability:

- *"… any trust assumption that can be violated to attack a system due to a flaw in an asset's design, implementation, or operation and management*."
- Vulnerabilities enable the attacker to infiltrate the system through one or more assets and pose a threat.*"*

O-RAN Specific Vulnerabilities
Unauthorized access to O-DU, O-CU and O-RU
Unprotected S-Plane and C-Plane in OFH interface
Disabling over-the-air cyphers for eavesdropping
Near-RT RIC conflicts with E2 nodes
xApp and rApp conflicts
xApp and rApp access to subscriber data:
Unprotected management interfaces
Injection of control messages to attack the U-Plane:

\Orchestrating a brighter world

O-RAN Risk Analysis

		Likelihood		
		Low	Medium	High
Severity	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider		+		+	+	+		+				+		+	+	+		+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
User		+		+	+	+		+				+		+	+	+		+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
Insider	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+	+	+		
Cloud operator	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+	+	+		
RAN operator	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+				
	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				+			+	+	+	+		

- The risk analysis has revealed that **medium to high security risks** can be identified in **numerous** interfaces and components specified in the context of O-RAN
- It is important that security improvements are included in the specification now to avoid the security weaknesses that occurred in the development of the 3GPP standards.

"Open RAN Risk Analysis", Barkhausen Institut, 2022

\Orchestrating a brighter world

O-RAN Risk Treatment

WP11's Risk Treatment: Work in Progress

Mitigation actions:

- Modify the Risk
  - Taking proactive measures to reduce the likelihood or impact of a threat
- Avoid the Risk
  - Stopping the activities that lead to the risk
- Share the Risk
  - Outsourcing the risk management to a third party
- Retain the Risk
  - Accepting the risk when the cost of mitigating it is higher than the potential impact

i2cat
\Orchestrating a brighter world NEC

NEC’s O-RAN Security White Paper

- “… principles such as openness and interoperability not only contribute to a better security …” “… but facilitate the adoption of well established security best practices …”

	Open RAN	Cloud RAN	Legacy RAN
Interfaces and protocols	Openly specified communication between Core Network and RAN, between Distributed Unit (DU) and Centralized Unit (CU), and between Radio Unit (RU) and Distributed Unit, based on 3GPP and O-RAN Alliance specifications	Openly specified communication between Core Network and RAN, and between Distributed Unit (DU) and Centralized Unit (CU) based on 3GPP specifications	Openly specified communication between Core Network and RAN based on 3GPP specifications
Security controls	Use of open protocols and tooling allows integration with centralized, third-party security controls, e.g., for identity management, logging, etc.; Open technology and cloud platform also enables adoption of established IT security best practices	Largely proprietary, except 3GPP-defined network security protocols; centralized solutions usually dependent on components supplied by the RAN technology vendor; cloud platform may provide certain centralized security controls	Largely proprietary, except 3GPP-defined network security protocols; centralized solutions usually dependent on components supplied by the RAN technology vendor
Compute platform	Cloud platform may be managed and configured by the MNO based on established best practices; virtualization layer may need to be optimized for software supplied by the RAN technology vendor.	Cloud platform may be managed and configured by the MNO based on established best practices; virtualization layer may need to be optimized for software supplied by the RAN technology vendor.	Closed hardware platform provided by the RAN technology vendor
Secure development and integration	Development is up to the RAN technology vendor, solution integration performed by MNO or specialized third party; MNO can test and validate compliance of individual solution components	Development and integration are up to the RAN technology vendor; MNO may support cloud deployment, but has limited ability to test individual solution components	Development and integration are up to the RAN technology vendor; MNO has limited ability to test security of individual solution components
Security operations	Use of *de facto* standard IT tools allows for increased visibility, enables intelligent RAN optimization using xApps/rApps, and makes it easier to adopt established security best practices	RAN software relies on proprietary tools provided by the RAN technology vendor; platform may be managed by MNO	Entire RAN deployment relies proprietary tools provided by the RAN technology vendor
Updates and security patches	May be tested and rolled-out by the MNO independently; unless directly related to RAN software, no RAN vendor dependency	Dependency on the RAN vendor who is required to test and release patches to RAN software and platform	Dependency on the RAN vendor who is required to test and release patches to RAN software and platform

In terms of Security, not everything coming from O-RAN are disadvantages

“Open RAN Security Examined”, NEC White Paper, 2022

\Orchestrating a brighter world

O-RAN Security Recommendations

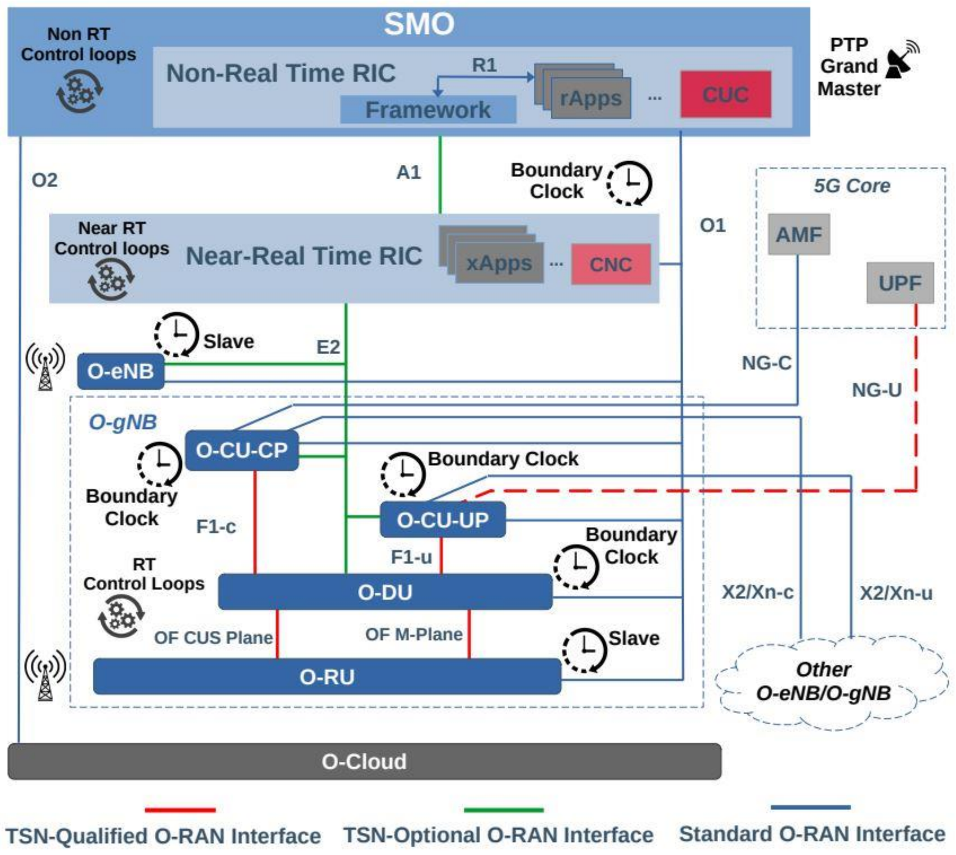
O-RAN allow for an increase of system security and availability:

- Strict Traffic Engineering
- AI-based anomaly detection systems
- Secured Provisioning and Certificate Enrollment
- Secure failure-proof virtualization of O-RAN
- Migration to Standalone 5G
- S-Plane attacks mitigation

“Open RAN Risk Analysis”, Barkhausen Institut, 2022

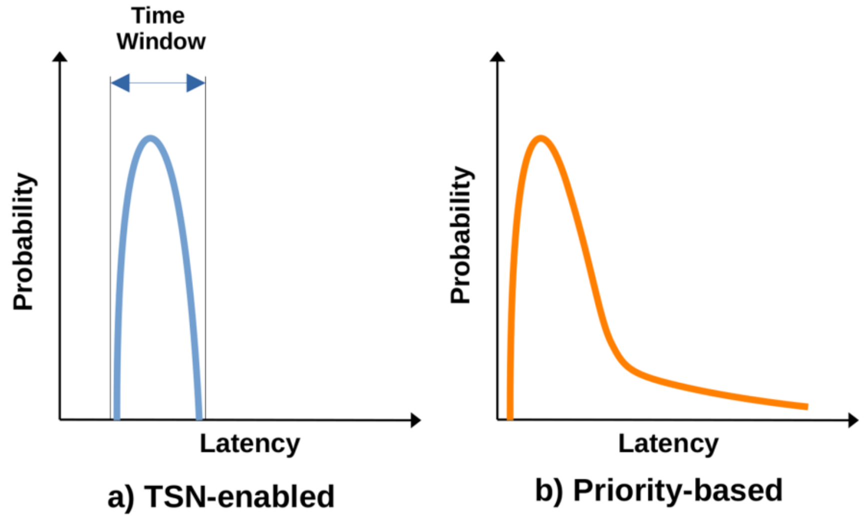
i2cat
\Orchestrating a brighter world NEC

Strict traffic engineering on a disaggreagated RAN to increase security:
Analysis of Latency-Critical Communication Interfaces



One of the O-RAN goals is to reduce costs to operators:

- General-purpose Ethernet networks can be shared to reduce costs: ''*crosshaul concept*''
- Time Sensitive Networking (TSN) can help to transport critical traffic in O-RAN interfaces
- TSN may also help to strictly isolate malicious flows in high latency-sensitive O-RAN interfaces (e.g., OFH)



Strict traffic engineering on a disaggreagated RAN to increase security:
Analysis of Latency-Critical Communication Interfaces

	Max. Delay	Max. FLR	Encapsulation	Ethernet	PON WDM	DOCSIS	Microwave	mmWave	TSN Qualified	TSN Optional
OF C	1 ms	10^{-7}	VLAN/eCPRI	Yes	Yes	No	No	Yes	✓	
OF U	25 μs - 1 ms	10^{-7}	VLAN/eCPRI	Yes	Yes	No	No	Yes	✓	
OF S	25 μs - 500 μs	10^{-7}	VLAN/PTP	Yes	Yes	No	No	Yes	✓	
OF M	100 ms	10^{-6}	VLAN/NETCONF	Yes	Yes	Yes	Yes	Yes		✓
F1-c	1.5-10 ms	N/A	VLAN/F1AP	Yes	Yes	Yes (LLX)	Yes	Yes	✓	
F1-u	1.5-10 ms	N/A	VLAN/GTP-U	Yes	Yes	Yes (LLX)	Yes	Yes	✓	
E2	10 ms	N/A	VLAN/E2AP	Yes	Yes	Yes (LLX)	Yes	Yes		✓
A1	500 ms	N/A	VLAN/A1AP	Yes	Yes	Yes	Yes	Yes		✓
NG-U	1-50ms	N/A	VLAN/GTP-U	Yes	Yes	Yes	Yes	Yes		✓

IEEE Communications Standards Magazine

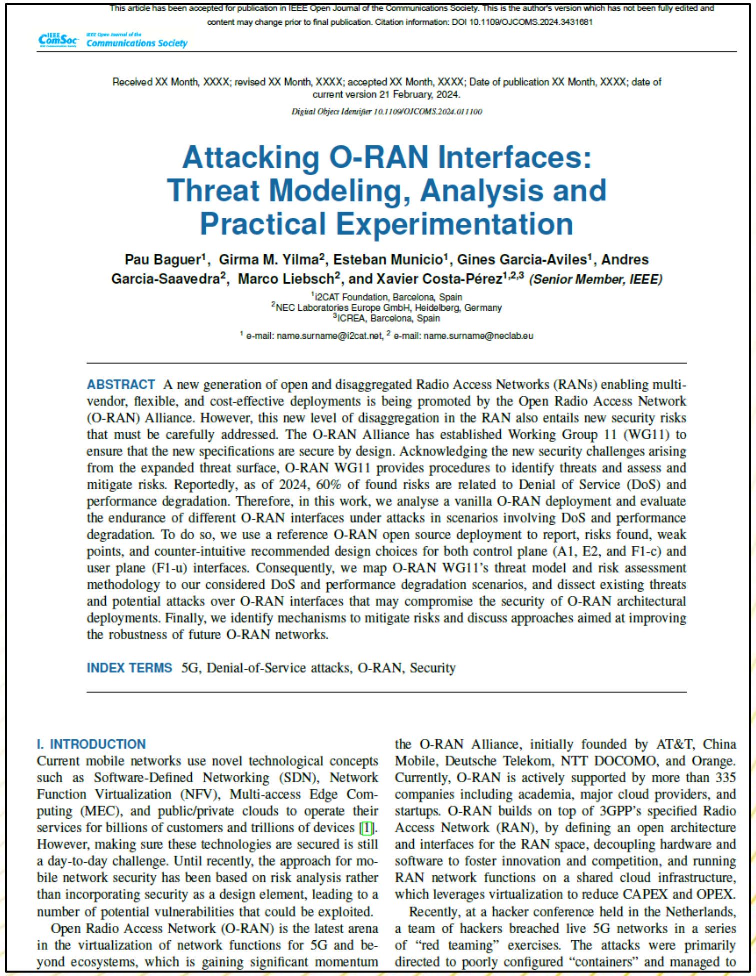
JOURNAL OF LaTeX CLASS FILES, VOL. 14, NO. 8, AUGUST 2015 1

O-RAN: Analysis of Latency-critical Interfaces and Overview of Time Sensitive Networking Solutions

Esteban Municio, Gines Garcia-Aviles, Andres Garcia-Saavedra and Xavier Costa-Pérez

Municio, E., Garcia-Aviles, G., Garcia-Saavedra, A., & Costa-Pérez, X. (2023). O-RAN: Analysis of Latency-Critical Interfaces and Overview of Time Sensitive Networking Solutions. *IEEE Communications Standards Magazine*, *7*(3), 82-89.

Attacking O-RAN Interfaces



This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2024.3431681

IEEE ComSoc IEEE Open Journal of the Communications Society

Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version 21 February, 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.011100

Attacking O-RAN Interfaces: Threat Modeling, Analysis and Practical Experimentation

Pau Baguer[1], Girma M. Yilma[2], Esteban Municio[1], Gines Garcia-Aviles[1], Andres Garcia-Saavedra[2], Marco Liebsch[2], and Xavier Costa-Pérez[1,2,3] (Senior Member, IEEE)

[1]i2CAT Foundation, Barcelona, Spain
[2]NEC Laboratories Europe GmbH, Heidelberg, Germany
[3]ICREA, Barcelona, Spain

[1] e-mail: name.surname@i2cat.net, [2] e-mail: name.surname@neclab.eu

ABSTRACT A new generation of open and disaggregated Radio Access Networks (RANs) enabling multi-vendor, flexible, and cost-effective deployments is being promoted by the Open Radio Access Network (O-RAN) Alliance. However, this new level of disaggregation in the RAN also entails new security risks that must be carefully addressed. The O-RAN Alliance has established Working Group 11 (WG11) to ensure that the new specifications are secure by design. Acknowledging the new security challenges arising from the expanded threat surface, O-RAN WG11 provides procedures to identify threats and assess and mitigate risks. Reportedly, as of 2024, 60% of found risks are related to Denial of Service (DoS) and performance degradation. Therefore, in this work, we analyse a vanilla O-RAN deployment and evaluate the endurance of different O-RAN interfaces under attacks in scenarios involving DoS and performance degradation. To do so, we use a reference O-RAN open source deployment to report, risks found, weak points, and counter-intuitive recommended design choices for both control plane (A1, E2, and F1-c) and user plane (F1-u) interfaces. Consequently, we map O-RAN WG11's threat model and risk assessment methodology to our considered DoS and performance degradation scenarios, and dissect existing threats and potential attacks over O-RAN interfaces that may compromise the security of O-RAN architectural deployments. Finally, we identify mechanisms to mitigate risks and discuss approaches aimed at improving the robustness of future O-RAN networks.

INDEX TERMS 5G, Denial-of-Service attacks, O-RAN, Security

I. INTRODUCTION

Current mobile networks use novel technological concepts such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), Multi-access Edge Computing (MEC), and public/private clouds to operate their services for billions of customers and trillions of devices [1]. However, making sure these technologies are secured is still a day-to-day challenge. Until recently, the approach for mobile network security has been based on risk analysis rather than incorporating security as a design element, leading to a number of potential vulnerabilities that could be exploited.

Open Radio Access Network (O-RAN) is the latest arena in the virtualization of network functions for 5G and beyond ecosystems, which is gaining significant momentum the O-RAN Alliance, initially founded by AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, and Orange. Currently, O-RAN is actively supported by more than 335 companies including academia, major cloud providers, and startups. O-RAN builds on top of 3GPP's specified Radio Access Network (RAN), by defining an open architecture and interfaces for the RAN space, decoupling hardware and software to foster innovation and competition, and running RAN network functions on a shared cloud infrastructure, which leverages virtualization to reduce CAPEX and OPEX.

Recently, at a hacker conference held in the Netherlands, a team of hackers breached live 5G networks in a series of "red teaming" exercises. The attacks were primarily directed to poorly configured "containers" and managed to

- P. Baguer, G. Yilma, E. Municio, G. García-Avilés, A. García-Saavedra, M. Liebsch, X. Costa-Pérez, *"Attacking O-RAN Interfaces: Threat Modeling, Analysis and Practical Experimentation,"* in *IEEE Open Journal of the Communications Society*, doi: 10.1109/OJCOMS.2024.3431681. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10606000

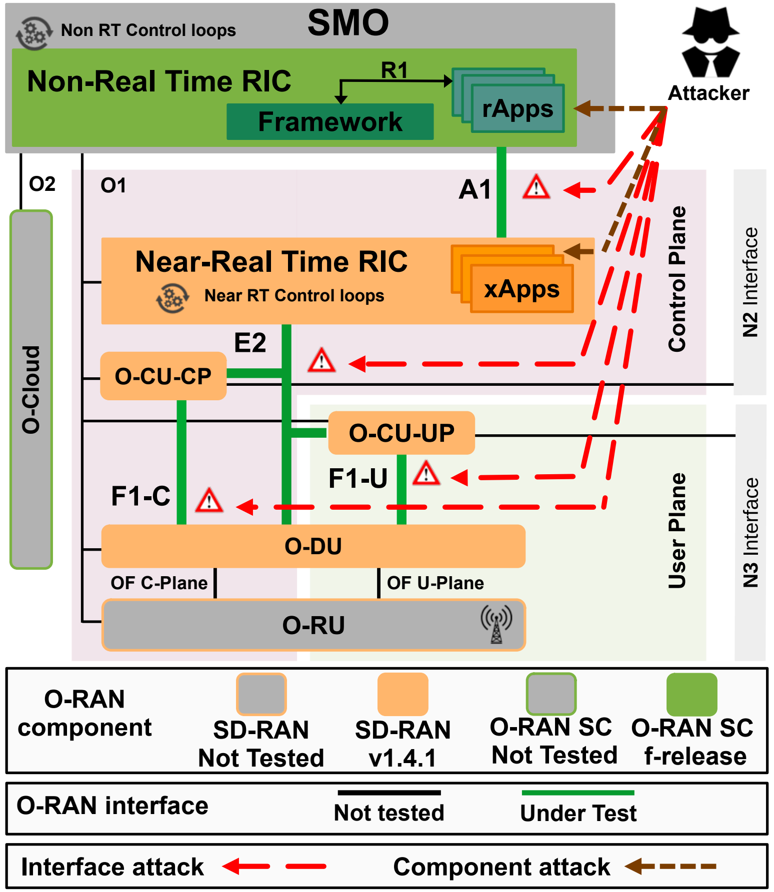
i2cat

Attacking O-RAN Interfaces: A Hands-on Analysis Through Performance Degradation

As of early 2023, over 60% of the vulnerabilities identified by the O-RAN Alliance WG11 in the previous categories mention DoS attacks and performance degradation attacks as direct or possible outcomes.

We measure the consequences of suffering attacks on:

- A1: Exchange of information and network policies between RICs
- E2: RAN monitoring and optimized control.
- F1-c: Control plane communication between O-CU and O-DU.
- F1-u: User plane communication between O-CU and O-DU.



Attacking O-RAN Interfaces: A Hands-on Analysis Through Performance Degradation

We consider three scenarios:

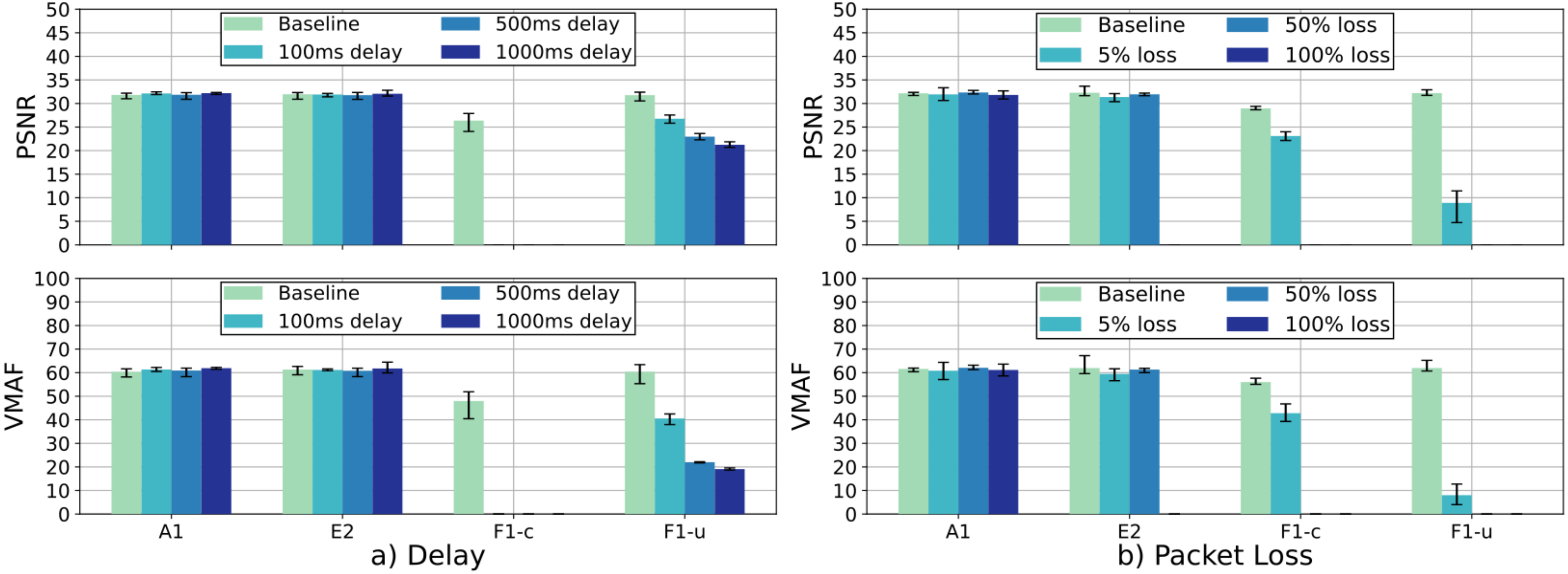
1. **<u>End-to-end Video Scenario:</u>** A UE from a network operator is requesting video-on-demand. Then, an attacker is able to harm operators' communications.
   - Exploited Surfaces: A1, E2, F1-c and F1-u communication interfaces.
   - KPI (U-Plane): Standardized QoE through the PSNR and VMAF
2. **<u>Policy-Based Slice Configuration Scenario:</u>** A RAN slice reconfiguration is triggered from the near-RT RIC, while a malicious attacker downgrades the control channel performance to delay the enforcement of this policy in the RAN.
   - Exploited Surfaces: E2 communication interface.
   - KPI (C-Plane): Policy reconfiguration timeliness within Operators' SLAs.
3. **<u>Subscriber Attachment Scenario:</u>** A UE is performing an attach procedure against the 5G core. Simultaneously, an attacker selectively degrades the performance of the control channels involving O-CUs and O-DUs, aiming to prevent users from attaching.
   - Exploited Surfaces: F1-c communication interface.
   - KPI (C-Plane): Successful Attach Rate of a UE performing the registration process (%).

THREAT ID	STUDIED INTERFACES			SCENARIOS		
	A1	E2	F1	1	2	3
T-O-RAN-01 near-RT RIC	✓	✓		✓	✓	
T-O-RAN-01 NonRT RIC + SMO	✓			✓		
T-O-RAN-01 O-CU		✓	✓	✓	✓	✓
T-O-RAN-01 O-DU		✓	✓	✓	✓	✓
T-O-RAN-02	✓	✓	✓	✓	✓	✓
T-O-RAN-03	✓	✓	✓	✓	✓	✓
T-O-RAN-05	✓	✓		✓	✓	
T-O-RAN-06	✓	✓	✓	✓	✓	✓
T-O-RAN-09	✓	✓	✓	✓	✓	✓
T-FRHAUL-01		✓	✓	✓	✓	✓
T-FRHAUL-02		✓	✓	✓	✓	✓
T-ORU-01-b			✓	✓		✓
T-NEAR-RT-02	✓	✓	✓	✓	✓	✓
T-NEAR-RT-03	✓	✓		✓	✓	
T-NEAR-RT-04	✓	✓		✓	✓	
T-NONRTRIC-01/03	✓			✓		
T-xAPP-01	✓	✓		✓	✓	
T-xAPP-03	✓	✓		✓	✓	
T-xApp-04	✓	✓		✓	✓	
T-rAPP-01	✓			✓		
T-rAPP-02	✓			✓		
T-rAPP-03	✓			✓		
T-rAPP-05	✓			✓		
T-PNF-01	✓	✓	✓	✓	✓	✓
T-SMO-03	✓			✓		
T-OPENSRC-02	✓	✓	✓	✓	✓	✓
T-PHYS-01/02	✓	✓	✓	✓	✓	✓
T-GEN-04	✓	✓	✓	✓	✓	✓
T-VM-C-01	✓	✓	✓	✓	✓	✓
T-VM-C-02	✓	✓	✓	✓	✓	✓
T-VM-C-04-a	✓	✓	✓	✓	✓	✓
T-VM-C-04-b	✓	✓	✓	✓	✓	✓
T-VM-C-05	✓	✓	✓	✓	✓	✓
T-IMG-04	✓	✓	✓	✓	✓	✓
T-VL-01	✓	✓	✓	✓	✓	✓
T-VL-03	✓	✓	✓	✓	✓	✓
T-O2-01	✓	✓	✓	✓	✓	✓
T-OCAPI-01	✓	✓	✓	✓	✓	✓

i2cat

Attacking O-RAN Interfaces: A Hands-on Analysis Through Performance Degradation

Some measured consequences:

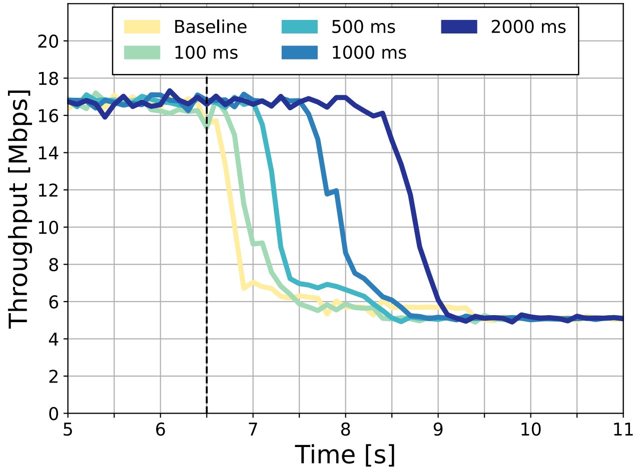


Attacking O-RAN Interfaces: A Hands-on Analysis Through Performance Degradation

Some measured consequences:

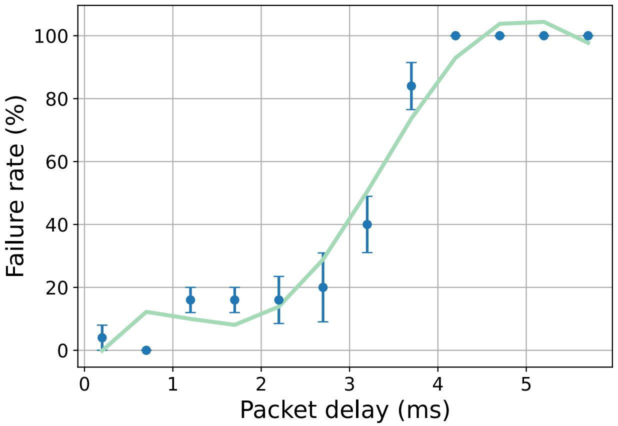
E2SM delayed policies

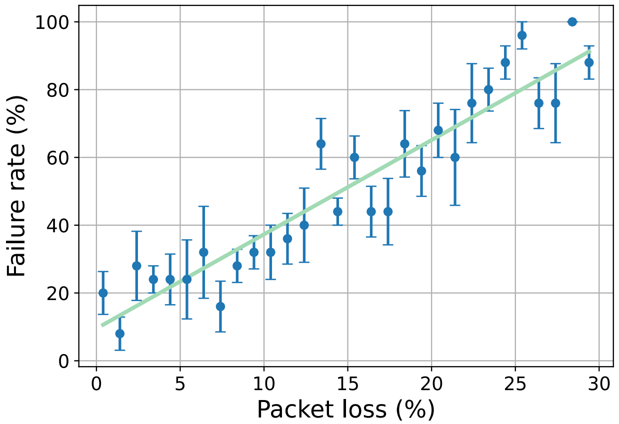
- Attacks in E2 will directly affect the time effectiveness of E2 policies.



Subscriber attachment success

- Attacks in F1-c are critical for control plane processes such as subscriber attachment.





Attacking O-RAN Interfaces: A Hands-on Analysis Through Performance Degradation

Interface	Service	Reaction to delays		Reaction to losses		Recovery
		Low ($d \geq$ 100ms)	High ($d \geq$ 2s)	Low ($e \geq 5\%$)	High ($e \geq 50\%$)	
A1	Interface	✓	✓	✓	✲	◷
	A1-P	✓	✓	✓	✲	◷
E2	Interface	✓	✓	✓	✓	✲
	onos-kpimon xApp	✓	✓	✓	✓	✗
	onos-rsm xApp	✓	✗	✓	✗	✗
F1-u	Interface	✓	✓	✓	✓	✲
F1-c	Interface	✗	✗	%	✗	✗
	UE attach.	✗	✗	%	✗	✗
	UE reconfig.	✗	✗	✗	✗	✗

✓ Unaffected | ✲ Temporarily unavailable | ◷ Slow recovery (∼5 min) | % High failure chance (∼20%) | ✗ Failure

Attacking O-RAN Interfaces: Main takeaways

DoS and performance degradation attacks on the O-RAN interfaces may have important impacts on overall RAN stability and security.

- F1-c is one of the most critical interfaces since some control messages have a maximum tolerated latency of about 3 ms.
- Delay and packet loss in the E2 may lead to ineffective policy enforcement and underperforming metric monitoring
- Performance degradation on F1-u only affects the user plane
- A1 is the least affected interface since it is expected that works in an non-RT regime
- Some xApps (e.g., rsm and kpimon) show instabilities and low recovery times after severe degradations

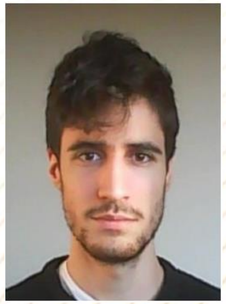
5G and O-RAN Security Review Towards 6G

Security and Privacy attacks on Cellular Networks

Part 2: Open Radio Access Networks (O-RAN)

Practice

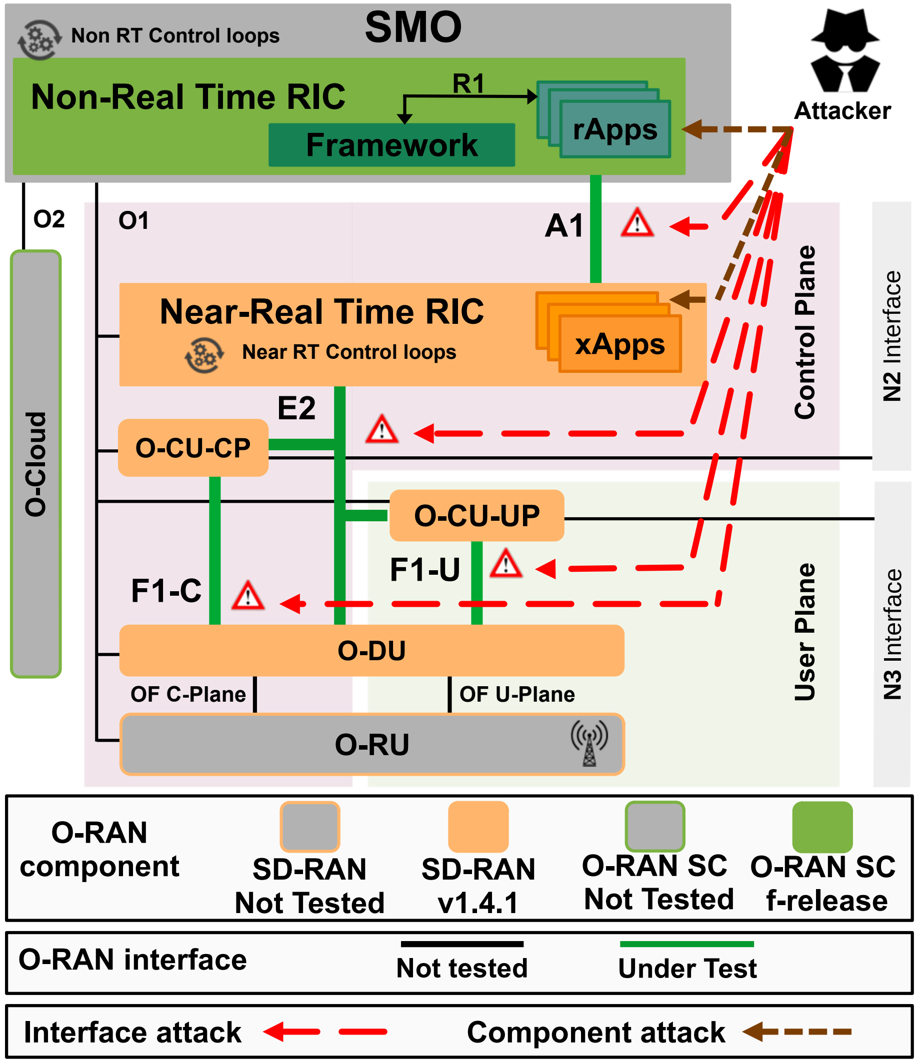
Pau
Baguer



Óscar
Lasierra

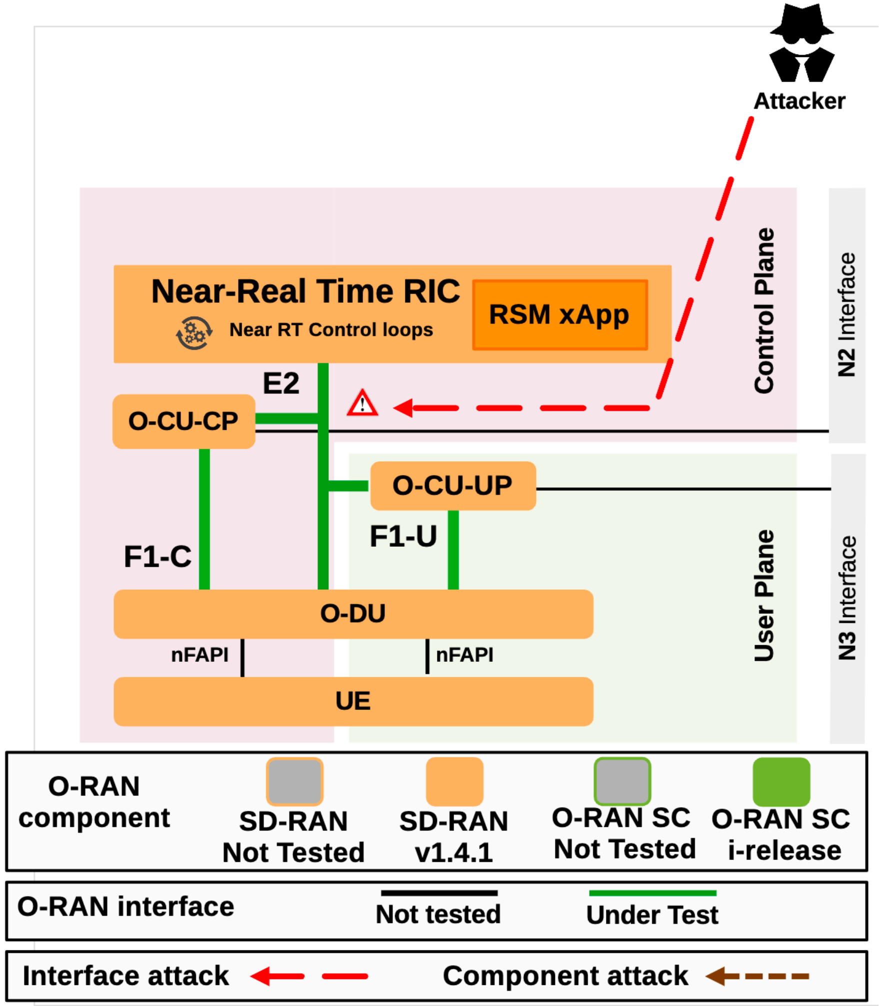
Full O-RAN deployment

- Non-RT RIC from O-RAN SC f-release
- Near-RT RIC from SD-RAN v1.4.1
- O-CU and O-DU from OpenAirInterface with SD-RAN E2 Agent
- UE-DU communication through nFAPI, bypassing L1



Schema of E2 interface demo: RAN Slice Management

- Data plane resources managed by RAN Slice Management (RSM)
- Data steam in the downlink direction
- Attack in the E2 interface



First data plane test: ping public addresses

```
*** T1: Internal network test: ping 192.168.250.1 (Internal router IP) ***
PING 192.168.250.1 (192.168.250.1) from 172.250.255.254 oaitun_ue1: 56(84) bytes of data.
64 bytes from 192.168.250.1: icmp_seq=1 ttl=64 time=20.4 ms
64 bytes from 192.168.250.1: icmp_seq=2 ttl=64 time=15.9 ms
64 bytes from 192.168.250.1: icmp_seq=3 ttl=64 time=15.8 ms

--- 192.168.250.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 15.796/17.393/20.443/2.157 ms
*** T2: Internet connectivity test: ping to 8.8.8.8 ***
PING 8.8.8.8 (8.8.8.8) from 172.250.255.254 oaitun_ue1: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=62.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=61.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=60.2 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 60.194/61.076/62.058/0.764 ms
*** T3: DNS test: ping to google.com ***
PING google.com (216.58.211.206) from 172.250.255.254 oaitun_ue1: 56(84) bytes of data.
64 bytes from mad01s25-in-f14.1e100.net (216.58.211.206): icmp_seq=1 ttl=113 time=48.6 ms
64 bytes from mad01s25-in-f14.1e100.net (216.58.211.206): icmp_seq=2 ttl=113 time=74.3 ms
64 bytes from mad01s25-in-f14.1e100.net (216.58.211.206): icmp_seq=3 ttl=113 time=46.2 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 46.178/56.341/74.271/12.716 ms
```

First data plane test: Iperf

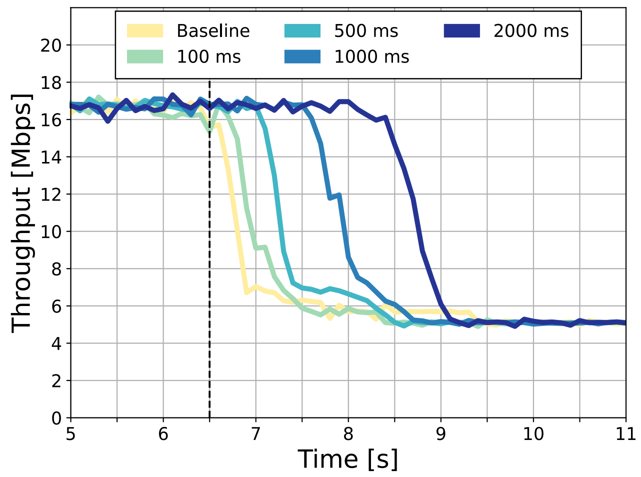
```
Server output:
Accepted connection from 192.168.250.1, port 39434
[  5] local 172.250.255.254 port 5001 connected to 192.168.250.1 port 37726
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  5]   0.00-1.00   sec  1.71 MBytes  14.3 Mbits/sec  0.764 ms  38/1272 (3%)  (omitted)
[  5]   1.00-2.00   sec  2.06 MBytes  17.2 Mbits/sec  0.642 ms  0/1487 (0%)  (omitted)
[  5]   0.00-1.00   sec  2.03 MBytes  17.0 Mbits/sec  2.327 ms  -38/1468 (-2.6%)
[  5]   1.00-2.00   sec  2.11 MBytes  17.7 Mbits/sec  0.648 ms  102/1625 (6.3%)
[  5]   2.00-3.00   sec  2.09 MBytes  17.5 Mbits/sec  0.642 ms  200/1712 (12%)
[  5]   3.00-4.00   sec  2.09 MBytes  17.6 Mbits/sec  0.654 ms  203/1718 (12%)
[  5]   4.00-5.00   sec  2.05 MBytes  17.2 Mbits/sec  4.754 ms  278/1763 (16%)
[  5]   5.00-6.00   sec  2.09 MBytes  17.6 Mbits/sec  0.639 ms  157/1672 (9.4%)
[  5]   6.00-7.00   sec  2.07 MBytes  17.4 Mbits/sec  0.616 ms  257/1753 (15%)
[  5]   7.00-8.00   sec  2.10 MBytes  17.6 Mbits/sec  0.656 ms  209/1726 (12%)
[  5]   8.00-9.00   sec  2.09 MBytes  17.6 Mbits/sec  0.701 ms  296/1810 (16%)
[  5]   9.00-10.00  sec  2.07 MBytes  17.4 Mbits/sec  0.637 ms  130/1628 (8%)
[  5]  10.00-11.00  sec  2.09 MBytes  17.6 Mbits/sec  0.640 ms  210/1725 (12%)
[  5]  11.00-12.00  sec  2.07 MBytes  17.4 Mbits/sec  5.938 ms  255/1753 (15%)
```

Create a slice of 30% of resources and move the UE to it

```
Server output:
Accepted connection from 192.168.250.1, port 45382
[  5] local 172.250.255.254 port 5001 connected to 192.168.250.1 port 49209
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  5]   0.00-1.00   sec  1.61 MBytes  13.5 Mbits/sec  0.648 ms  0/1164 (0%)  (omitted)
[  5]   1.00-2.00   sec  2.14 MBytes  18.0 Mbits/sec  0.662 ms  0/1551 (0%)  (omitted)
[  5]   0.00-1.00   sec  2.10 MBytes  17.6 Mbits/sec  0.670 ms  0/1520 (0%)
[  5]   1.00-2.00   sec  2.10 MBytes  17.6 Mbits/sec  1.589 ms  141/1662 (8.5%)
[  5]   2.00-3.00   sec  2.10 MBytes  17.7 Mbits/sec  0.631 ms  143/1665 (8.6%)
[  5]   3.00-4.00   sec  2.10 MBytes  17.6 Mbits/sec  0.656 ms  180/1699 (11%)
[  5]   4.00-5.00   sec   865 KBytes  7.09 Mbits/sec  2.312 ms  102/713 (14%)
[  5]   5.00-6.00   sec   656 KBytes  5.37 Mbits/sec  2.812 ms  469/932 (50%)
[  5]   6.00-7.00   sec   654 KBytes  5.36 Mbits/sec  3.289 ms  1256/1718 (73%)
[  5]   7.00-8.00   sec   656 KBytes  5.37 Mbits/sec  9.699 ms  1401/1864 (75%)
[  5]   8.00-9.00   sec   656 KBytes  5.37 Mbits/sec  2.646 ms  1134/1597 (71%)
[  5]   9.00-10.00  sec   647 KBytes  5.30 Mbits/sec  3.109 ms  1255/1712 (73%)
[  5]  10.00-11.00  sec   656 KBytes  5.37 Mbits/sec  9.752 ms  1400/1863 (75%)
[  5]  11.00-12.00  sec   656 KBytes  5.37 Mbits/sec  2.647 ms  1132/1595 (71%)
[  5]  12.00-13.00  sec   656 KBytes  5.37 Mbits/sec  2.840 ms  1255/1718 (73%)
```

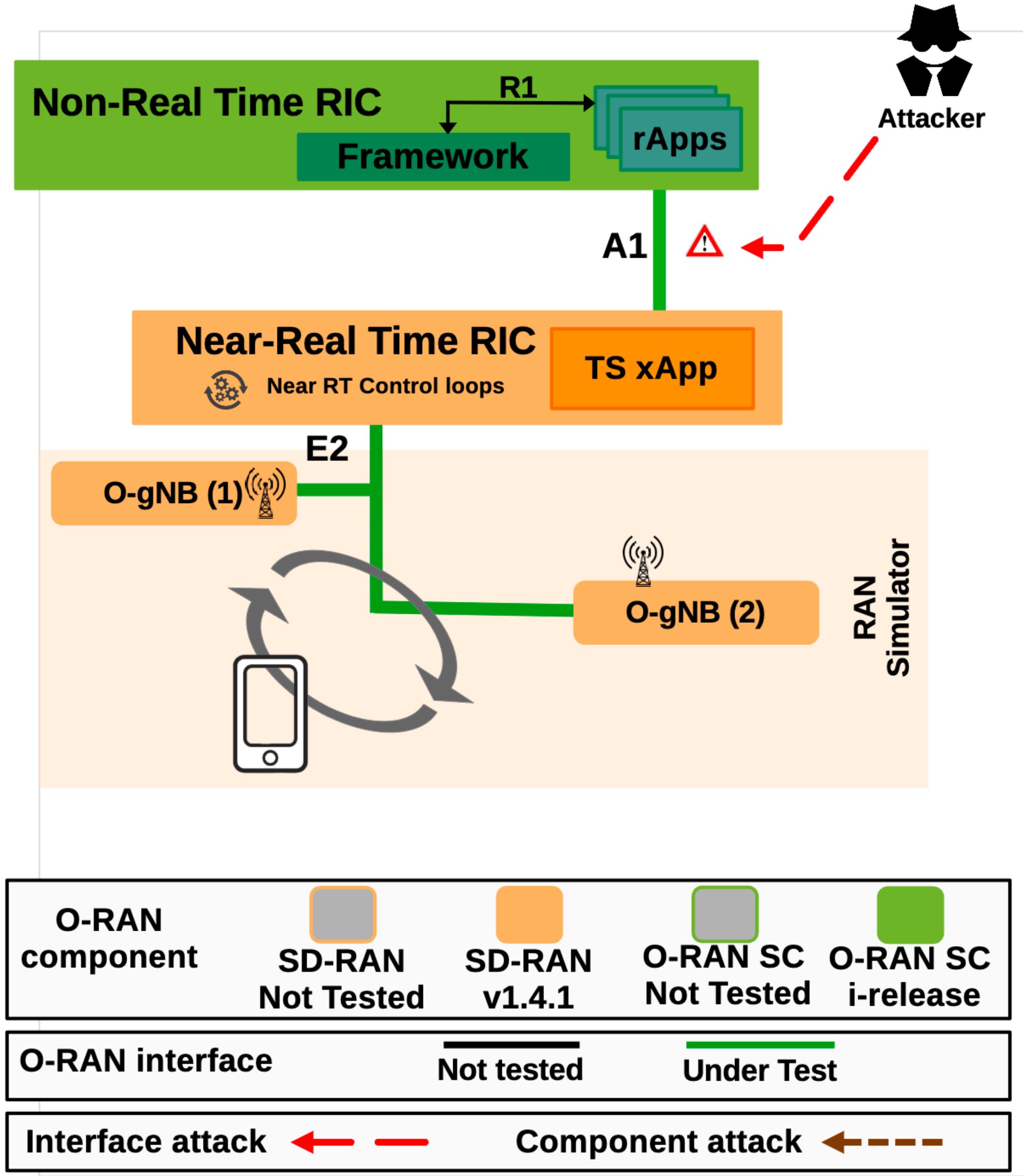
Consequences of a DoS attack

```
Server output:
Accepted connection from 192.168.250.1, port 59390
[  5] local 172.250.255.254 port 5001 connected to 192.168.250.1 port 37706
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  5]   0.00-1.00   sec  1.71 MBytes  14.3 Mbits/sec  1.947 ms  0/1234 (0%)  (omitted)
[  5]   1.00-2.00   sec  2.10 MBytes  17.7 Mbits/sec  0.632 ms  0/1522 (0%)  (omitted)
[  5]   0.00-1.00   sec  2.10 MBytes  17.6 Mbits/sec  0.634 ms  0/1521 (0%)
[  5]   1.00-2.00   sec  2.09 MBytes  17.5 Mbits/sec  0.656 ms  24/1536 (1.6%)
[  5]   2.00-3.00   sec  2.10 MBytes  17.6 Mbits/sec  0.664 ms  191/1712 (11%)
[  5]   3.00-4.00   sec  2.10 MBytes  17.7 Mbits/sec  0.631 ms  235/1757 (13%)
[  5]   4.00-5.00   sec  2.09 MBytes  17.6 Mbits/sec  0.663 ms  191/1704 (11%)
[  5]   5.00-6.00   sec  2.10 MBytes  17.7 Mbits/sec  0.636 ms  202/1724 (12%)
[  5]   6.00-7.00   sec  1.01 MBytes  8.43 Mbits/sec  2.374 ms  90/817 (11%)
[  5]   7.00-8.00   sec   651 KBytes  5.34 Mbits/sec  3.031 ms  362/822 (44%)
[  5]   8.00-9.00   sec   656 KBytes  5.37 Mbits/sec  3.554 ms  1385/1848 (75%)
[  5]   9.00-10.00  sec   656 KBytes  5.37 Mbits/sec  2.639 ms  1150/1613 (71%)
[  5]  10.00-11.00  sec   654 KBytes  5.36 Mbits/sec  2.841 ms  1253/1715 (73%)
[  5]  11.00-12.00  sec   656 KBytes  5.37 Mbits/sec  3.118 ms  1255/1718 (73%)
[  5]  12.00-13.00  sec   656 KBytes  5.37 Mbits/sec  3.586 ms  1390/1853 (75%)
```

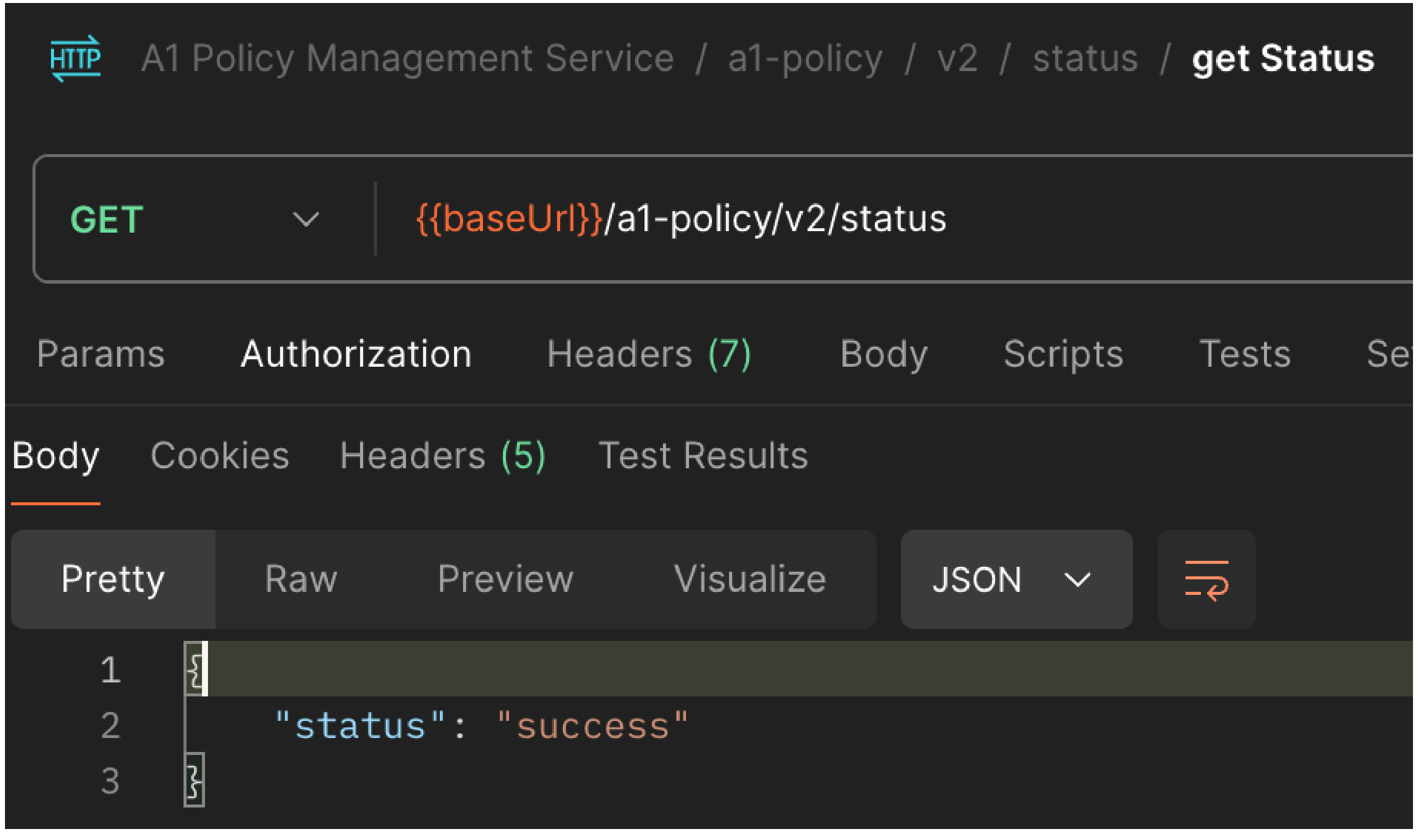


Schema of A1 interface demo

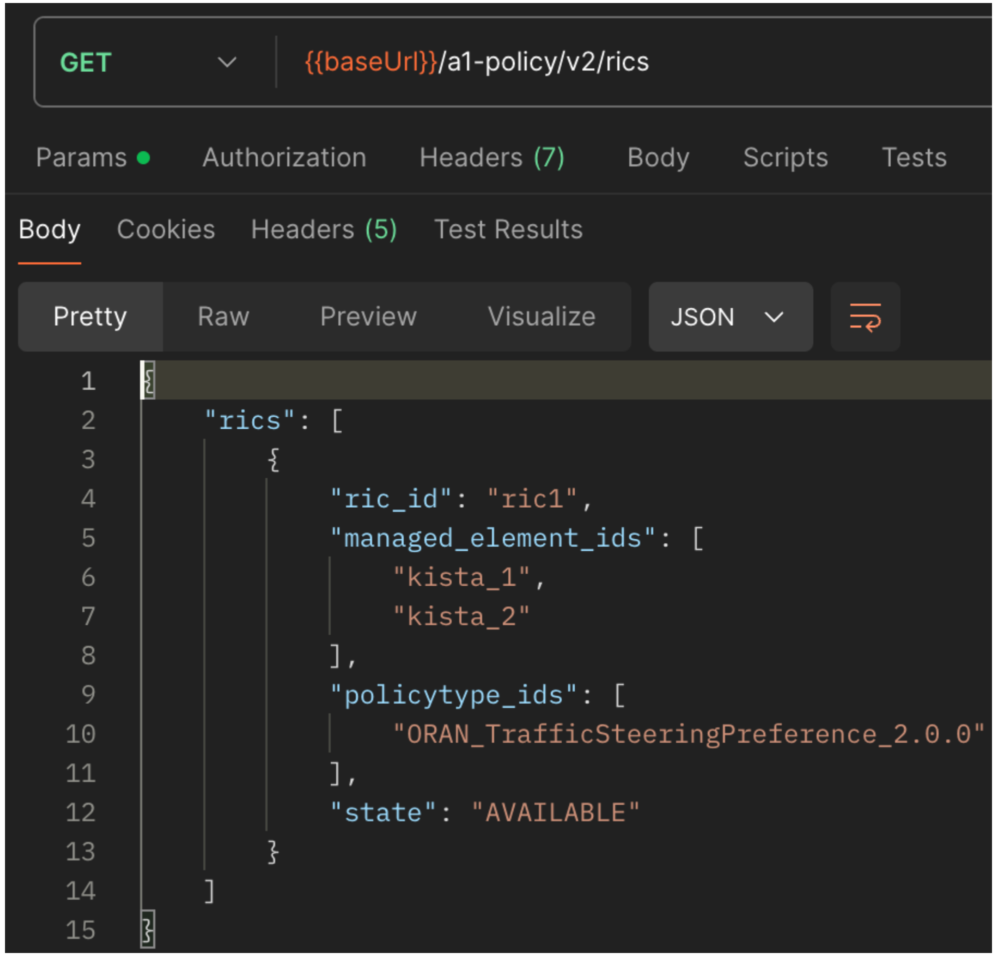
- Mobility managed by Traffic steering (TS) xApp.
- Policies are created in A1 to manage the TS xApp.
- The UE is 'physically moving' and being handovered based on the best RSRP (cell with the best coverage).
- Attack in the A1 interface



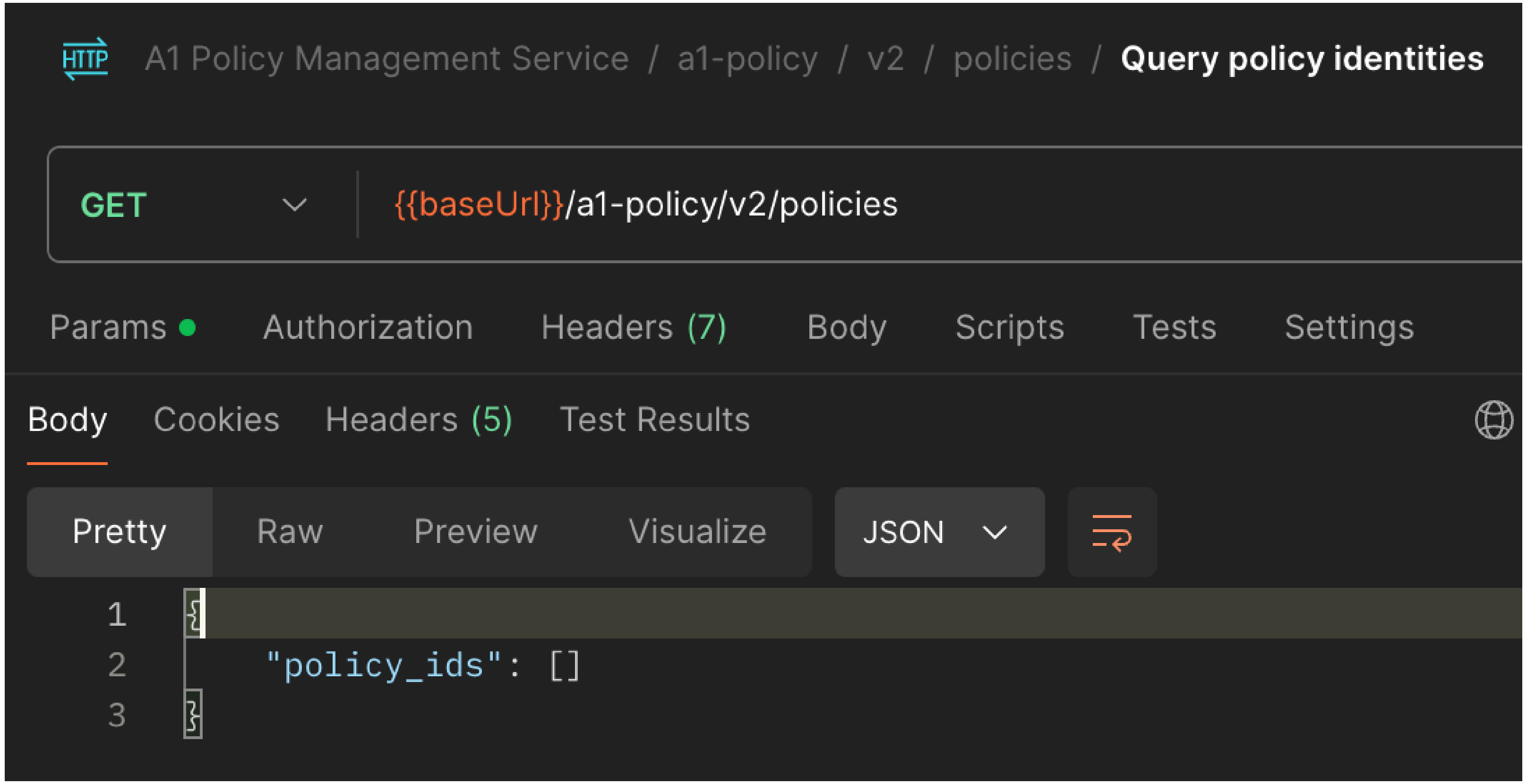
Query non-RT RIC A1 interface status



Query non-RT RIC A1 interface connections



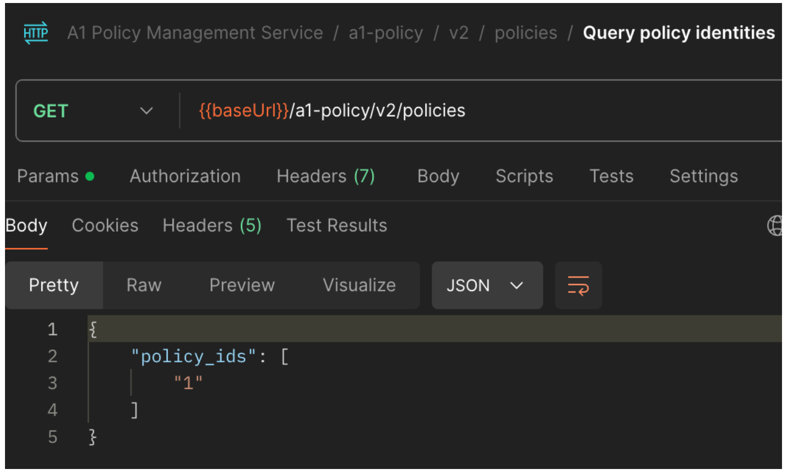
Query non-RT RIC's active A1 policies

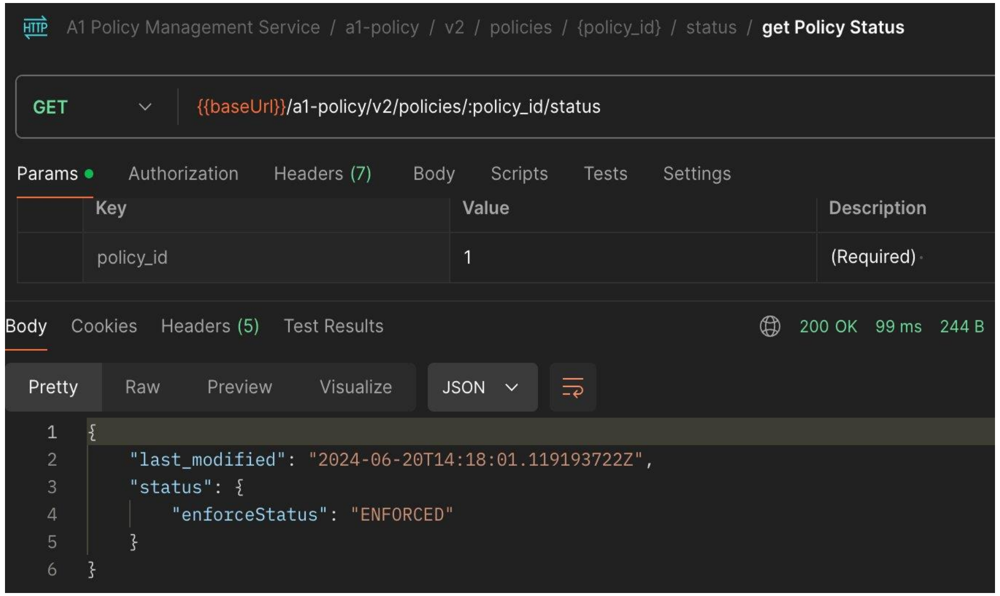


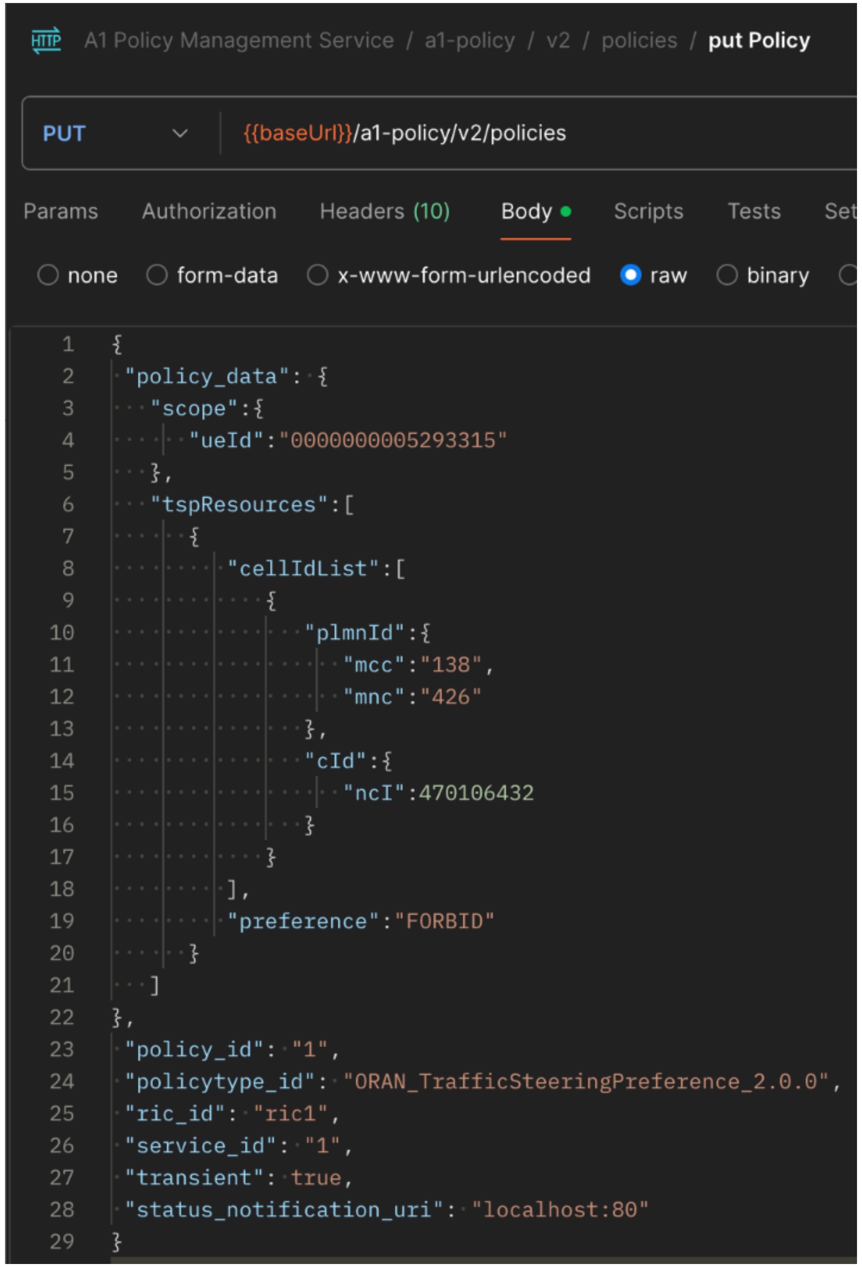
UE is being handovered based on the cell with best RSRP

```
2024-06-23T22:17:00.498Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ──────────────────── CELLS ────────────────────
2024-06-23T22:17:00.498Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5153/1454c001 CGI:13842601c054140 UEs:[]
2024-06-23T22:17:00.498Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[3086191]
2024-06-23T22:17:00.498Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:462
2024-06-23T22:17:00.498Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ──────────────────── UES ────────────────────
2024-06-23T22:17:00.498Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:502  ID:3086191 STATUS:CONNECTED 5QI: 2 CGI:138426010055140 CGIs(RSRP): [138426010055140 (-104) 13842601c054140 (-116)]
2024-06-23T22:17:00.498Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:506
2024-06-23T22:17:03.510Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:419
2024-06-23T22:17:03.510Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ──────────────────── CELLS ────────────────────
2024-06-23T22:17:03.510Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5153/1454c001 CGI:13842601c054140 UEs:[]
2024-06-23T22:17:03.510Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[3086191]
2024-06-23T22:17:03.510Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:462
2024-06-23T22:17:03.510Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ──────────────────── UES ────────────────────
2024-06-23T22:17:03.510Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:502  ID:3086191 STATUS:CONNECTED 5QI: 2 CGI:138426010055140 CGIs(RSRP): [138426010055140 (-108) 13842601c054140 (-114)]
2024-06-23T22:17:03.510Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:506
2024-06-23T22:17:06.520Z    INFO    rimedo-ts/sdran/manager sdran/manager.go:312    CONTROL MESSAGE: UE [ID:0000000003086191, 5QI:2] switched between CELLs [CGI:138426010055140 → CGI:13842601c054140

2024-06-23T22:17:06.525Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:419
2024-06-23T22:17:06.525Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ──────────────────── CELLS ────────────────────
2024-06-23T22:17:06.525Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5153/1454c001 CGI:13842601c054140 UEs:[3086191]
2024-06-23T22:17:06.525Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[]
2024-06-23T22:17:06.525Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:462
2024-06-23T22:17:06.525Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ──────────────────── UES ────────────────────
2024-06-23T22:17:06.525Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:502  ID:3086191 STATUS:CONNECTED 5QI: 2 CGI:13842601c054140 CGIs(RSRP): [138426010055140 (-112) 13842601c054140 (-111)]
2024-06-23T22:17:06.525Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:506
2024-06-23T22:17:09.541Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:419
2024-06-23T22:17:09.541Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ──────────────────── CELLS ────────────────────
2024-06-23T22:17:09.541Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5153/1454c001 CGI:13842601c054140 UEs:[3086191]
2024-06-23T22:17:09.541Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[]
2024-06-23T22:17:09.541Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:462
2024-06-23T22:17:09.541Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ──────────────────── UES ────────────────────
2024-06-23T22:17:09.541Z    DEBUG   rimedo-ts/ts-manager    manager/manager.go:502  ID:3086191 STATUS:CONNECTED 5QI: 2 CGI:13842601c054140 CGIs(RSRP): [138426010055140 (-114) 13842601c054140 (-108)]
```

Creation of an A1 policy







Creation of an A1 policy

```
DEBUG  rimedo-ts/ts-manager  manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[9106040]
DEBUG  rimedo-ts/ts-manager  manager/manager.go:462
DEBUG  rimedo-ts/ts-manager  manager/manager.go:571  ------------------------------------------------------------ UES ------------------------------------------------------------
DEBUG  rimedo-ts/ts-manager  manager/manager.go:502  ID:9106040 STATUS:CONNECTED 5QI: 2 CGI:138426010055140 CGIs(RSRP): [138426010055140 (-114) 13842601c054140 (-108)]
DEBUG  rimedo-ts/ts-manager  manager/manager.go:506
DEBUG  rimedo-ts/ts-manager  manager/manager.go:321
DEBUG  rimedo-ts/ts-manager  manager/manager.go:571  ---------------------------------------------------------- POLICIES ----------------------------------------------------------
DEBUG  rimedo-ts/ts-manager  manager/manager.go:395  ID:1 POLICY: {UE [ID:9106040] - (FORBID) - CELL [CGI:13842601c054140]} STATUS: ENFORCED
DEBUG  rimedo-ts/ts-manager  manager/manager.go:399
DEBUG  rimedo-ts/ts-manager  manager/manager.go:419
DEBUG  rimedo-ts/ts-manager  manager/manager.go:571  ----------------------------------------------------------- CELLS -----------------------------------------------------------
DEBUG  rimedo-ts/ts-manager  manager/manager.go:449  ID:e2:1/5153/1454c001 CGI:13842601c054140 UEs:[]
DEBUG  rimedo-ts/ts-manager  manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[9106040]
DEBUG  rimedo-ts/ts-manager  manager/manager.go:462
DEBUG  rimedo-ts/ts-manager  manager/manager.go:571  ------------------------------------------------------------ UES ------------------------------------------------------------
DEBUG  rimedo-ts/ts-manager  manager/manager.go:502  ID:9106040 STATUS:CONNECTED 5QI: 2 CGI:138426010055140 CGIs(RSRP): [138426010055140 (-111) 13842601c054140 (-111)]
DEBUG  rimedo-ts/ts-manager  manager/manager.go:506
DEBUG  rimedo-ts/ts-manager  manager/manager.go:321
DEBUG  rimedo-ts/ts-manager  manager/manager.go:571  ---------------------------------------------------------- POLICIES ----------------------------------------------------------
DEBUG  rimedo-ts/ts-manager  manager/manager.go:395  ID:1 POLICY: {UE [ID:9106040] - (FORBID) - CELL [CGI:13842601c054140]} STATUS: ENFORCED
DEBUG  rimedo-ts/ts-manager  manager/manager.go:399
DEBUG  rimedo-ts/ts-manager  manager/manager.go:419
DEBUG  rimedo-ts/ts-manager  manager/manager.go:571  ----------------------------------------------------------- CELLS -----------------------------------------------------------
DEBUG  rimedo-ts/ts-manager  manager/manager.go:449  ID:e2:1/5153/1454c001 CGI:13842601c054140 UEs:[]
DEBUG  rimedo-ts/ts-manager  manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[9106040]
DEBUG  rimedo-ts/ts-manager  manager/manager.go:462
DEBUG  rimedo-ts/ts-manager  manager/manager.go:571  ------------------------------------------------------------ UES ------------------------------------------------------------
DEBUG  rimedo-ts/ts-manager  manager/manager.go:502  ID:9106040 STATUS:CONNECTED 5QI: 2 CGI:138426010055140 CGIs(RSRP): [138426010055140 (-108) 13842601c054140 (-114)]
DEBUG  rimedo-ts/ts-manager  manager/manager.go:506
```

Creation of an A1 policy

```
DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[9106040]
DEBUG   rimedo-ts/ts-manager    manager/manager.go:462
DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ---------------------------------------------------- UES ----------------------------------------------------
DEBUG   rimedo-ts/ts-manager    manager/manager.go:502  ID:9106040 STATUS:CONNECTED 5QI: 2 CGI:138426010055140 CGIs(RSRP): [138426010055140 (-114) 13842601c054140 (-108)]
DEBUG   rimedo-ts/ts-manager    manager/manager.go:506
DEBUG   rimedo-ts/ts-manager    manager/manager.go:321
DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  -------------------------------------------------- POLICIES --------------------------------------------------
DEBUG   rimedo-ts/ts-manager    manager/manager.go:395  ID:1 POLICY: {UE [ID:9106040] - (FORBID) - CELL [CGI:13842601c054140]} STATUS: ENFORCED
DEBUG   rimedo-ts/ts-manager    manager/manager.go:399
DEBUG   rimedo-ts/ts-manager    manager/manager.go:419
DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  --------------------------------------------------- CELLS ---------------------------------------------------
DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5153/1454c001 CGI:13842601c054140 UEs:[]
DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[9106040]
DEBUG   rimedo-ts/ts-manager    manager/manager.go:462
DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ---------------------------------------------------- UES ----------------------------------------------------
DEBUG   rimedo-ts/ts-manager    manager/manager.go:502  ID:9106040 STATUS:CONNECTED 5QI: 2 CGI:138426010055140 CGIs(RSRP): [138426010055140 (-111) 13842601c054140 (-111)]
DEBUG   rimedo-ts/ts-manager    manager/manager.go:506
DEBUG   rimedo-ts/ts-manager    manager/manager.go:321
DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  -------------------------------------------------- POLICIES --------------------------------------------------
DEBUG   rimedo-ts/ts-manager    manager/manager.go:395  ID:1 POLICY: {UE [ID:9106040] - (FORBID) - CELL [CGI:13842601c054140]} STATUS: ENFORCED
DEBUG   rimedo-ts/ts-manager    manager/manager.go:399
DEBUG   rimedo-ts/ts-manager    manager/manager.go:419
DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  --------------------------------------------------- CELLS ---------------------------------------------------
DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5153/1454c001 CGI:13842601c054140 UEs:[]
DEBUG   rimedo-ts/ts-manager    manager/manager.go:449  ID:e2:1/5154/14550001 CGI:138426010055140 UEs:[9106040]
DEBUG   rimedo-ts/ts-manager    manager/manager.go:462
DEBUG   rimedo-ts/ts-manager    manager/manager.go:571  ---------------------------------------------------- UES ----------------------------------------------------
DEBUG   rimedo-ts/ts-manager    manager/manager.go:502  ID:9106040 STATUS:CONNECTED 5QI: 2 CGI:138426010055140 CGIs(RSRP): [138426010055140 (-108) 13842601c054140 (-114)]
DEBUG   rimedo-ts/ts-manager    manager/manager.go:506
```

Consequences of a DoS attack

```json
{
    "rics": [
        {
            "ric_id": "ric1",
            "managed_element_ids": [
                "kista_1",
                "kista_2"
            ],
            "policytype_ids": [
                "ORAN_TrafficSteeringPreference_2.0.0"
            ],
            "state": "CONSISTENCY_CHECK"
        }
    ]
}
```

```json
{
    "rics": [
        {
            "ric_id": "ric1",
            "managed_element_ids": [
                "kista_1",
                "kista_2"
            ],
            "policytype_ids": [
                "ORAN_TrafficSteeringPreference_2.0.0"
            ],
            "state": "UNAVAILABLE"
        }
    ]
}
```

References

- O. Lasierra, G. Garcia-Aviles, E. Municio, A. Skarmeta, and X. Costa-Pérez, *“European 5G Security in the Wild: Reality versus Expectations”,* In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23). https://doi.org/10.1145/3558482.3581776 https://dl.acm.org/doi/abs/10.1145/3558482.3581776

- O. Lasierra, N. Ludant, G. Garcia-Aviles, E. Municio, G. Noubir, A. Skarmeta, X. Costa-Pérez, *“Unmasking 5G Security: Bridging the Gap Between Expectations and Reality”,* TechRxiv, to be published https://www.techrxiv.org/doi/full/10.36227/techrxiv.172055660.06334898

- P. Baguer, G. Yilma, E. Municio, G. García-Avilés, A. García-Saavedra, M. Liebsch, X. Costa-Pérez, *"Attacking O-RAN Interfaces: Threat Modeling, Analysis and Practical Experimentation,"* in *IEEE Open Journal of the Communications Society*, doi: 10.1109/OJCOMS.2024.3431681. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10606000

Tutorial: *"5G and O-RAN Security Review Towards 6G: Security and Privacy Attacks on Cellular Networks"*

First Summer School on Security and Privacy in 6G Networks

Universidad Complutense de Madrid

Madrid, June 24-28

Team: **Esteban Municio, Ginés García, Oscar Lasierra, Pau Baguer, Xavier Costa**

i2cat

Never stop designing the digital future

i2CAT.net

CERCA Centres de Recerca de Catalunya

tecnio catalonia ACCIÓ Generalitat de Catalunya