5G IMSI Catchers Mirage

Ravishankar Borgaonkar, SINTEF Digital & University of Stavanger
Altaf Shaik, TU Berlin

5 August 2021

IMSI Catchers / Stingrays / Fake Base Stations

- Fake devices simulating a part or complete cellular network
- Identification & tracking of mobile devices in the radio coverage are
- Interception of mobile user data & radio signalling data
- Battery drain / DoS / Kill switch / Downgrading to lower generation networks
- Silently affects mobile users privacy if misused illegally

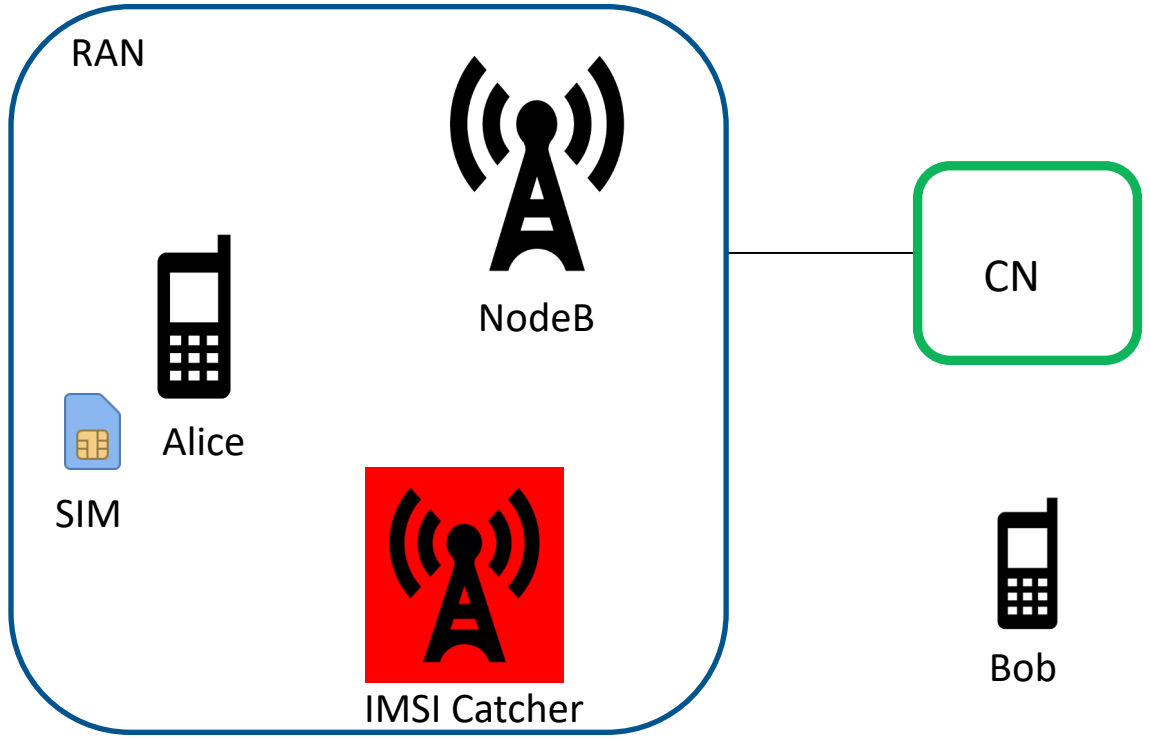
IMSI Catchers Types

- Passive
  - Less powerful as does not interact with mobile phones or networks
  - Silent (difficult to detect) to mobile users and networks
- Active
  - More powerful
  - Control mobiles phones as a master-slave architecture most of the time
  - Can be detected technically (**almost impossible on commercial devices**)

IMSI Catcher

4G Networks & 4G IMSI Catchers

- Exploit weaknesses in the cellular network security design
  - Device attach, authentication, & paging procedure
- Identities
  - IMSI
  - IMEI
  - Others if not correctly randomized by the network (TMSI/GUTI)



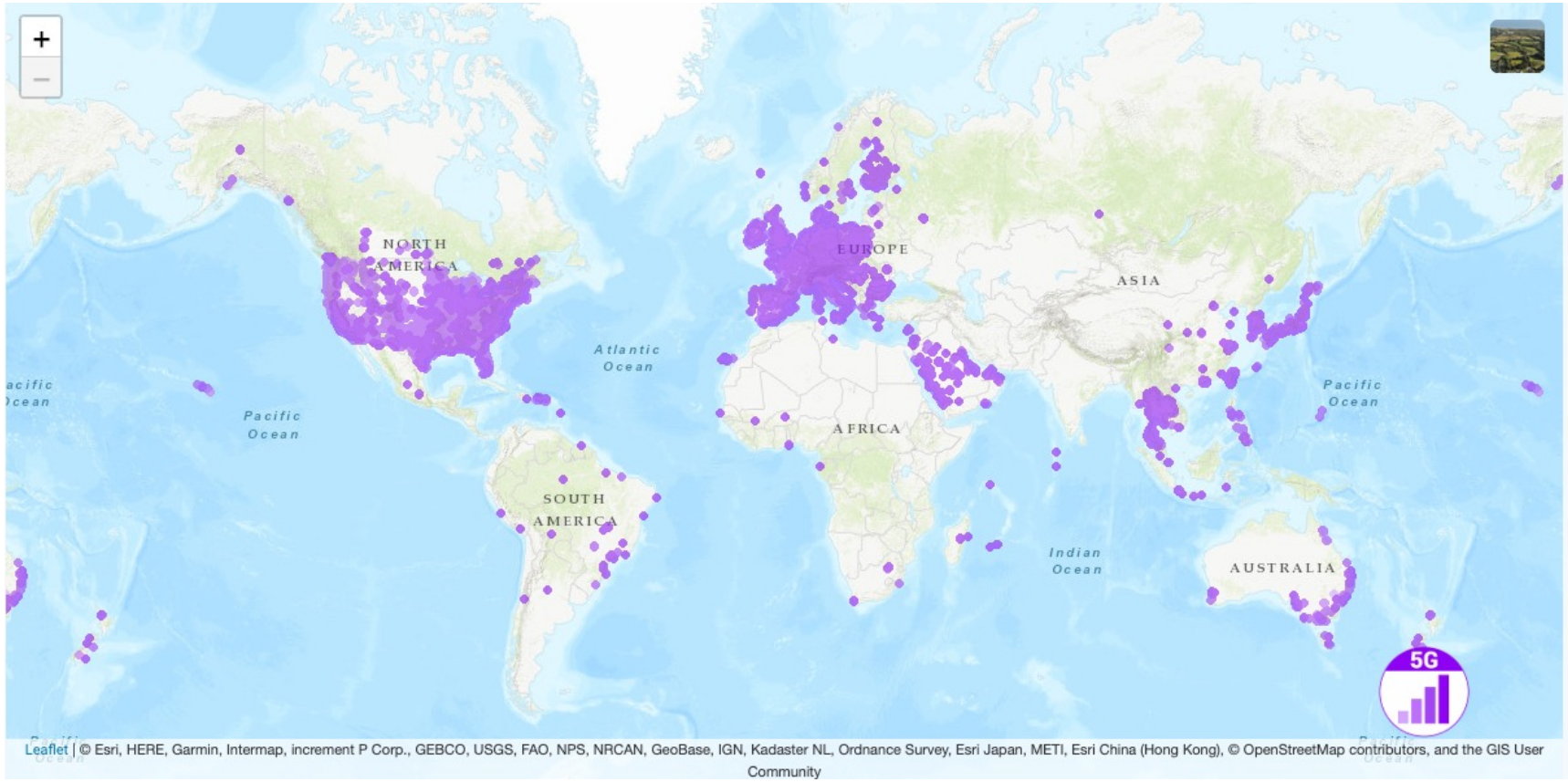
Note: picture provides an abstract view only. RAN – Radio Access Network CN – Core Network SIM- Subscriber Identity Module

SINTEF

5G Network & Radio Security Improvements

5G Networks

- Ultra-high speed (~1 GB)
- Ultra-low latency
- Ultra-low enegery for IoT
- ..
- Security features++



SINTEF

5G Deployment Types

2021

5G/4G towers

4G Core Network

Non-Standalone Mode

202?

5G towers

5G Core Network

Standalone Mode

SINTEF

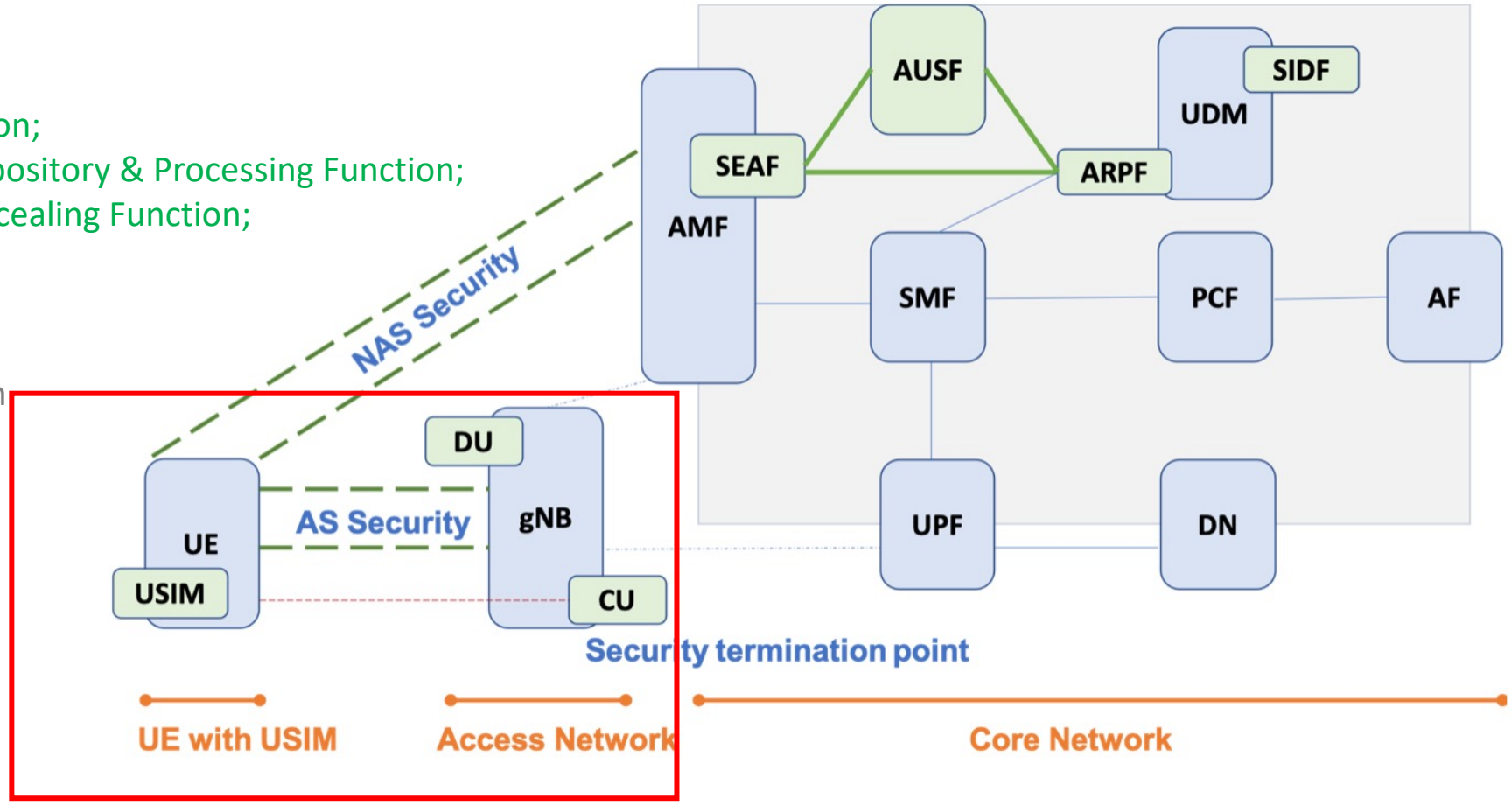
5G Security Architecture

gNB - NodeB
DU - Distributed Unit
CU - Central Unit

AUSF - AUthentication Server Function;
ARPF - Authentication credential Repository & Processing Function;
SIDF - Subscription Identifier De-concealing Function;
SEAF - SEcurity Anchor Function

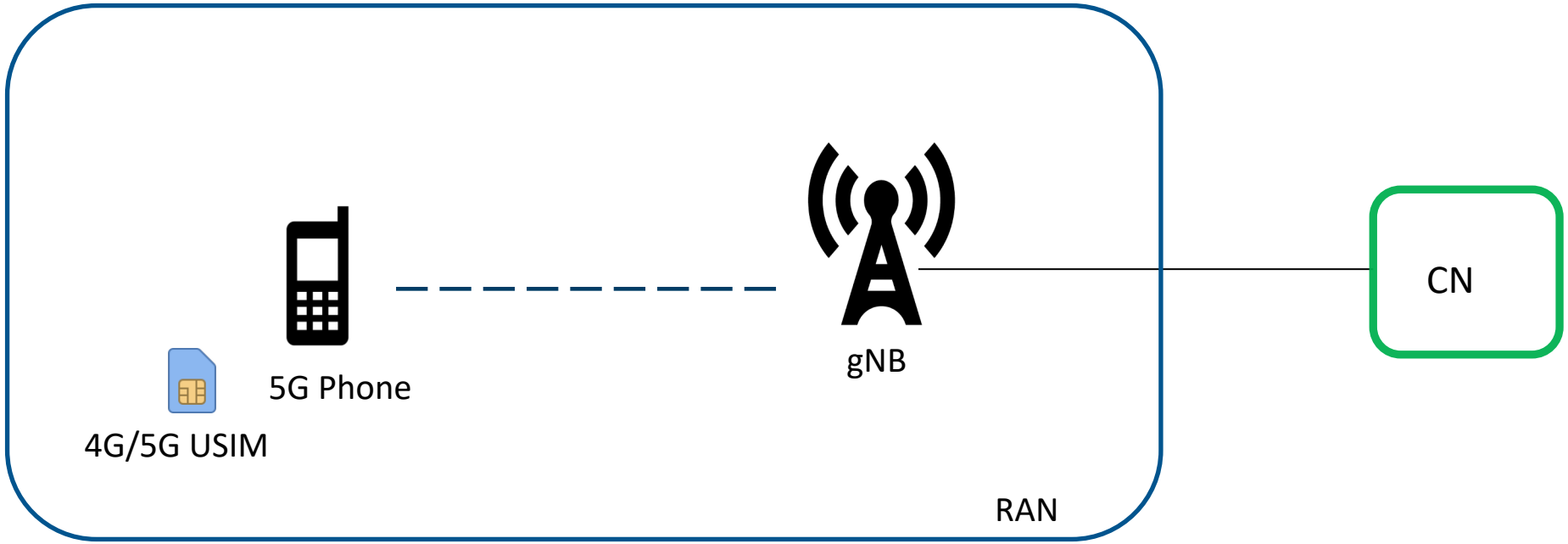
AMF - Access Management Function
SMF - Session Management Function
UDM - Unified Data Mandagement
PCF - Policy Control Function
AF- Application Function
UPF - User Plane Function
DN - Data Network

AS – Access Stratum
NAS – Non-access Stratum



5G RAN Security Features

- We focus on features reducing impact of IMSI catchers on mobile users



gNB : Next Generation NodeB – 5G base station

SINTEF

New Long Term 5G-Identity

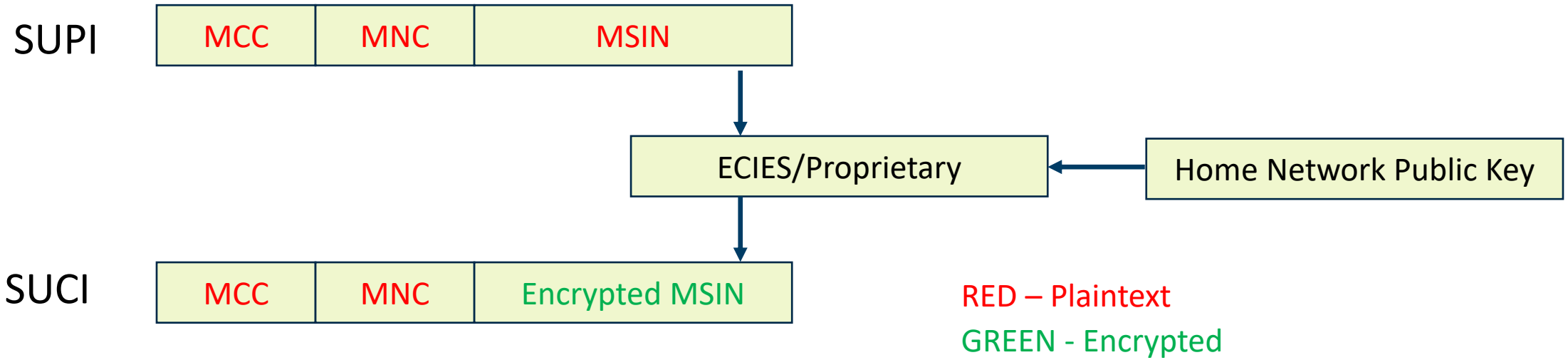
- SUPI – Subscription Permanent Identifier
- Confidentiality of subscriber identity
  - Home network public keys to protect SUPI
  - Encrypted SUPI == SUCI for authentication procedure
  - SUPI never transmitted OTA unless using legacy networks or “null scheme”
  - No paging by SUPI identifier
- Improved protection
  - Passive attacks (eavesdropping)
  - Active attacks (probing identify)

IMSI (4G)

SUPI (5G)

New Identifiers (SUPI + SUCI)

- SUPI – Subscription Permanent Identifier
- SUCI – Subscription Concealed Identifier (SU-SHI)
- Public key of the home network operator



SINTEF

5G Paging - I

- Improved 5G Paging procedure
- UE Paging occasion is derived from 5G-S-TMSI instead of IMSI
  - Prevents a passive attacker from determining 10 bits of IMSI (observing the paging occasion used by the UE)
  - In 4G, it is derived from IMSI
- Paging identifier must be 5G-S-TMSI or I-RNTI
  - In 4G, IMSI or S-TMSI

https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_103/Docs/R2-1812276.zip
https://3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_127_Sanya/Docs/S2-184332.zip

5G Paging - II

- Refreshens of temporary identifier in paging procedure

- Unlike in 4G, **mandatory** to refresh 5G-S-TMSI after paging
  - As optional feature in 4G, GUTI is same even for 3 days

The AMF shall support assigning 5G-GUTI to the UE.

The AMF shall support reallocating 5G-GUTI to UE.

https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_88_Dali/docs/S3-171783.zip

Shot Term Temporary 5G-Identifier

- 5G-GUTI : Globally Unique Temporary Identifier
- Mandatory to refresh 5G-GUTI
- Improved privacy protection
  - Passive attacks (eavesdropping)
  - Active attacks

GUTI (4G)

5G-GUTI (5G)

Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE, the AMF shall send a new 5G-GUTI to the UE in the registration procedure.

Upon receiving Registration Request message of type "periodic registration update" from a UE, the AMF should send a new 5G-GUTI to the UE in the registration procedure.

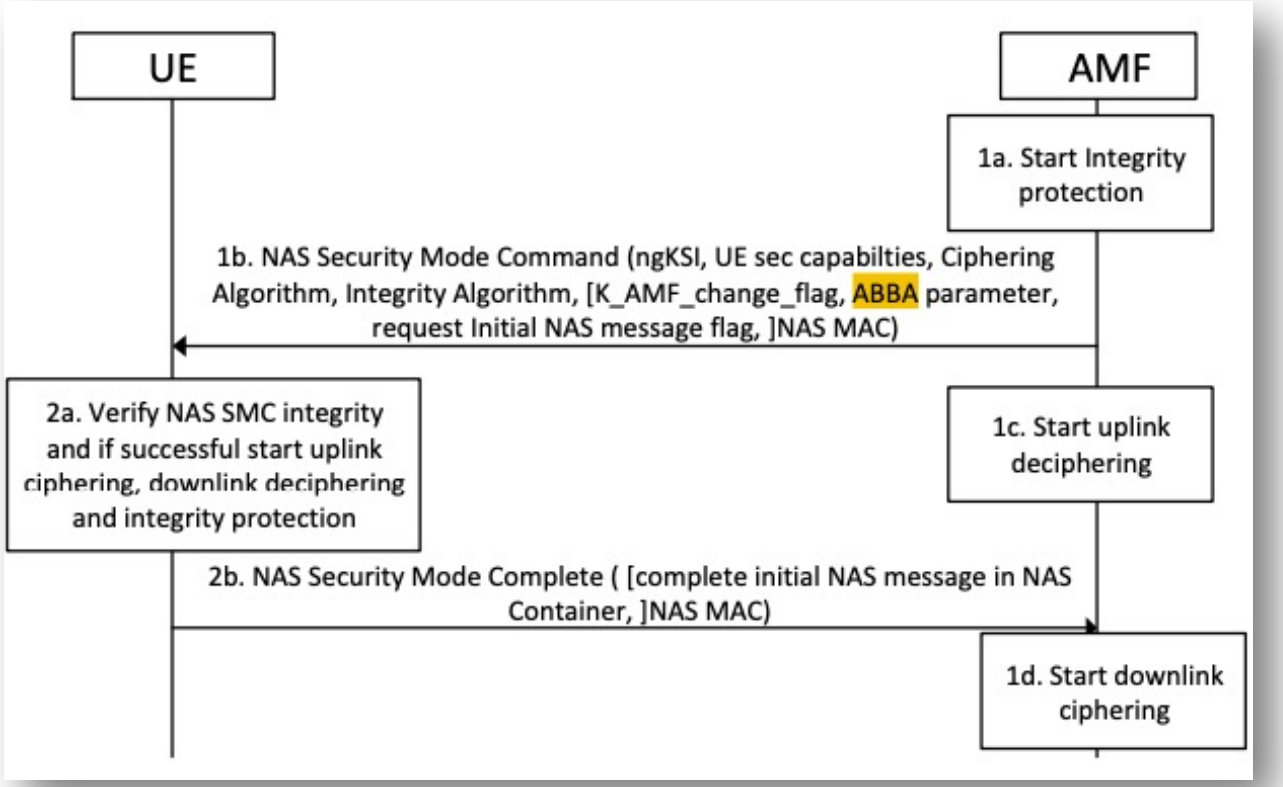
Upon receiving Service Request message sent by the UE in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released.

SINTEF

ABBA Parameter

- Anti Bidding down Between Architectures (ABBA)
- Protection of security features & indicates enabled security features of connected network
- Used during 5G AKA protocol versions
  - SEAF sets ABBA parameter while sending RAND, AUTN

ABBA(5G)



SINTEF

User Plane Integrity Protection

- User Plane communication between UE and the network

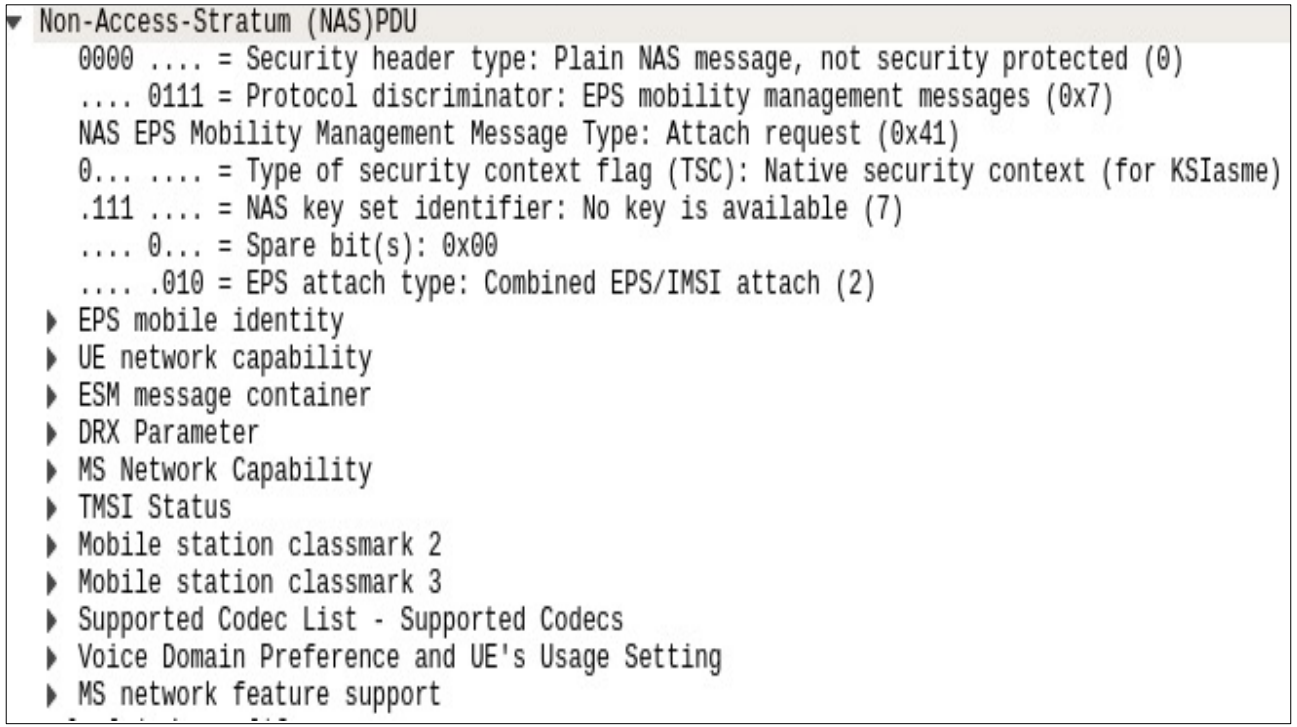
- Integrity protection for user plane traffic
  - In 4G, user data is not integrity protected

- However, not mandatory and optional to use
  - Determined by the network based on policy

https://alter-attack.net/

Secure UE Capability transfer

- UE capabilities are exchanged after security establishment
  - In 4G, it was not the case & possible to perfom MiTM attacks (DoS/Downgrading)



SINTEF

UE-assisted network-based IMSI catcher detection

- Use of UE measurement reports
  - Using existing mechanisms to detect fake base station and inconsistent information in the network
  - Not a bullet proof approach, but is a good start

E.2 Examples of using measurement reports

The received-signal strength and location information in measurement reports can be used to detect a false base station which attract the UEs by transmitting signal with higher power. They can also be used to detect a false base station which replays the genuine MIB/SIB without modification.

In order to detect a false base station which replays modified version of broadcast information to prevent victim UEs from switching back and forth between itself and genuine base stations (e.g. modifying neighbouring cells, cell reselection criteria, registration timers, etc. to avoid the so called ping-pong effect), information on broadcast information can be used to detect inconsistency from the deployment information.

Further, a false base station which uses inconsistent cell identifier or operates in inconsistent frequency than the deployment of the genuine base stations, can be detected respectively by using the cell identifier or the frequency information in the measurement reports.

Measurement reports collected from multiple UEs can be used to filter out incorrect reports sent by a potential rogue UE.

Upon detection of the false base station, the operator can take further actions, e.g. informing legal authorities or contacting the victim UE.

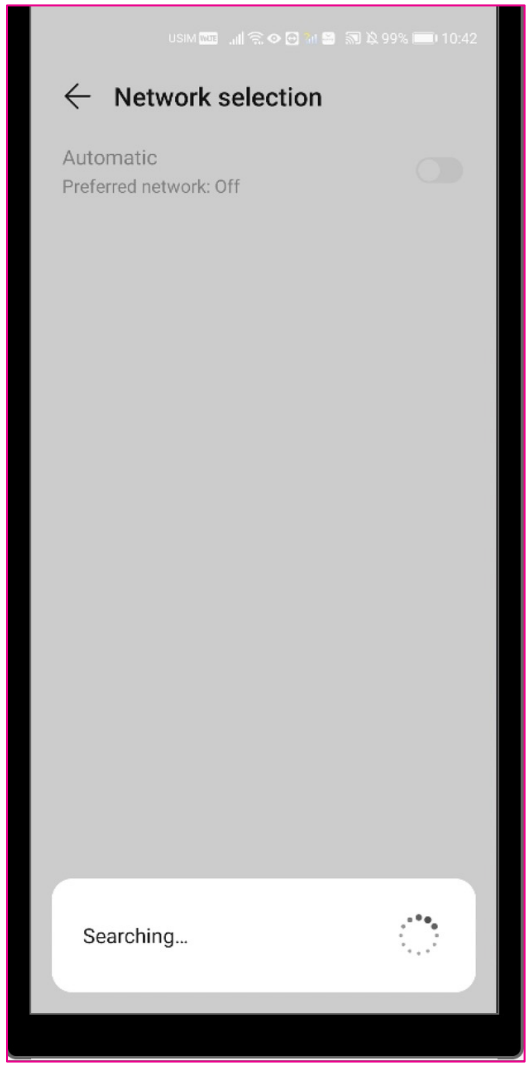
Annex E of TS 33.501 Release 15

Security Features Availability

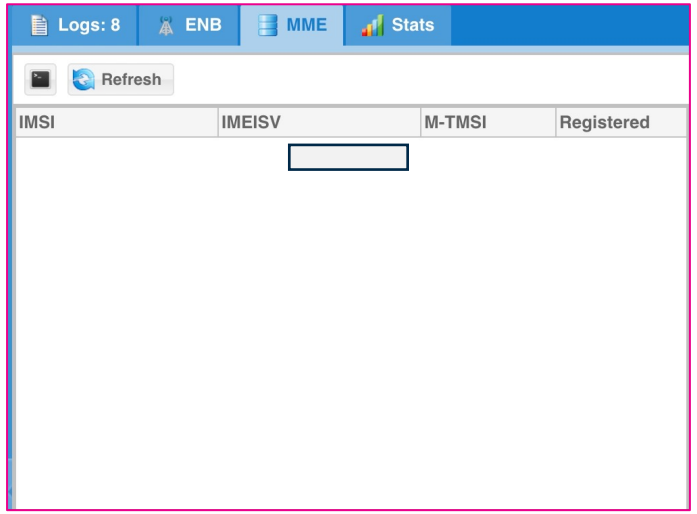
Security Features	5G NSA	5G SA
Encrypted SUPI	❌	✅
Mandatory Fresh 5G-GUTI reallocation	❌	✅
Paging by only 5G-S-TMSI	❌	✅
ABBA parameter	❌	✅
Integrity protection	❌	✅
UE-assisted Network based IMSI catcher detection	❌	✅
Secure UE capabilities transfer	✅	✅

5G IMSI Catchers - NSA

- IMSI is not encrypted -> exposed over-the-air
- No manadotry 4G-GUTI reallocation
- 4G core network, expect GUTI randomness
- Let's see real 5G NSA network data: Commercial and open source tools
  - Upto 4 NSA networks in 2 countries



Huawei P40 5G



Our Test 5G NSA Network

SINTEF

Tracking with GUTI – Operator 1

- Sufficiently randomized and updated periodically
  - 4G LTE network
    - 2015 vs 2021
  - 5G NSA network
    - 2021

Time	4G LTE 2015	4G LTE 2021	5G NSA 2021
10:00	0xadf02cd4	0xdd348782	0xdd082f96
11:00	0xadf12cd4	0xdd72392f	0xdd097b32
12:00	0xadf32cd4	0xdd0423de	0xdd823ef3
13:00	0xadf62cd4	0xdd639202	0xdd87663d
14:00	0xadf82cd4	0xdd63192f	0xdd84c782

Tracking with GUTI – Operator 2

- Does not change for a day sometimes
- Lack of randomness and refreshens (when user is not moving)
- Possible to link GUTI to a subscriber

Date	5G NSA
20 June	0xC1A2B000
25 June	0xC1A33000
2 July	0xC1A3F008
3 July	0xC1B23007
21 June	0xC1B4E001

Tracking with GUTI – Operator 3

- Does not change even after 10+ days
- Remains same after device restart or flight mode on/off

Date	5G NSA
24 June	0xF5863006
25 June	0xF5863006
2 July	0xF5863006
3 July	0xF5863006
6 July	0xF5863006

Frequently Refreshing GUTI

- Will prevent many other attacks: require internal policies and timers to activate this
- Can invoke Periodic TAU, with change of GUTI
  - Not observed in practice with data-enabled
- No GUTI reallocation command observed
  - GUTI remains same for whole day if Tracking area remains same (work location or home)
  - GUTI remains same after 50 rounds of calls and data transmission activities

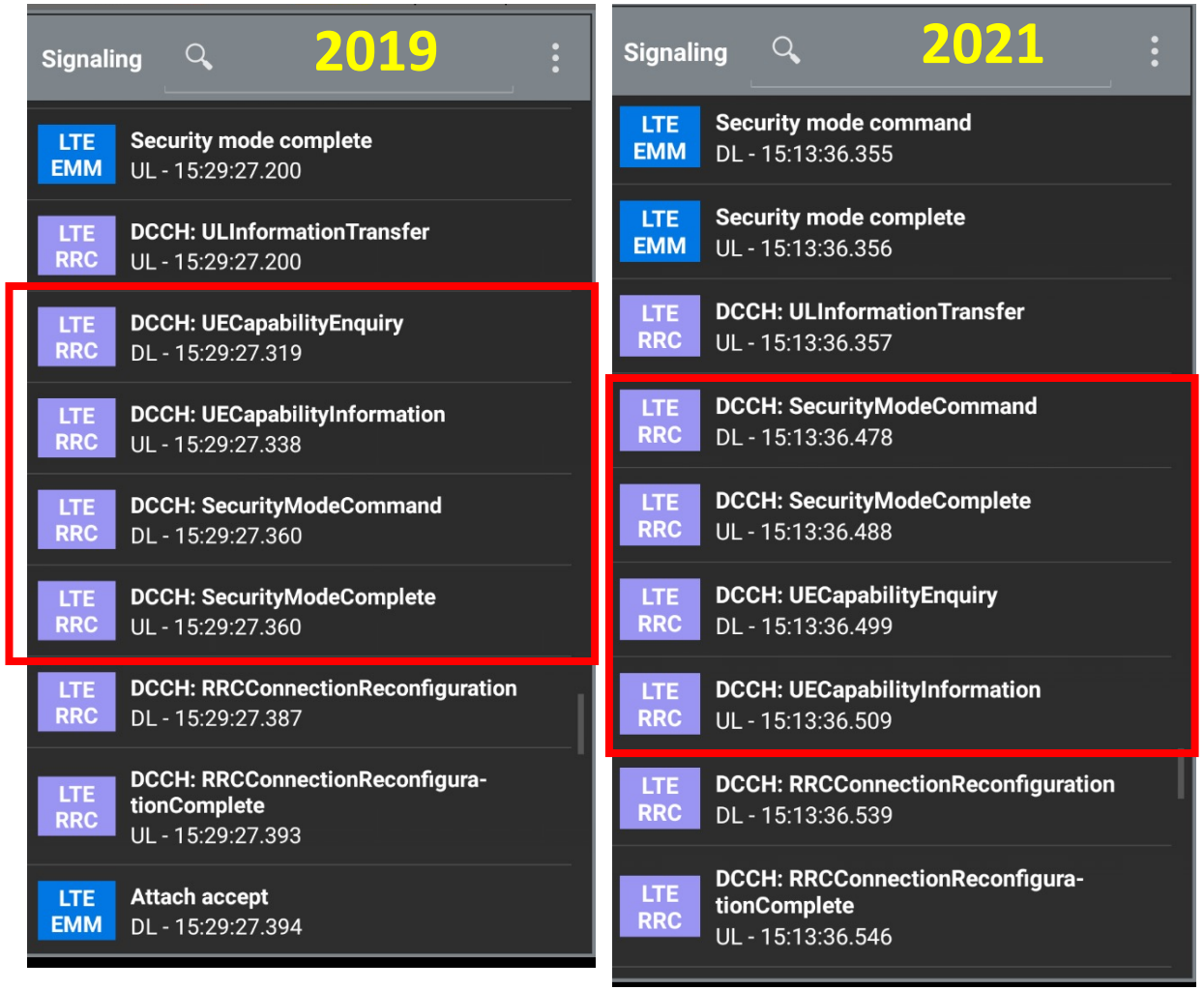
Downgrading to 3G/2G

- Downgrading attack still possible from active IMSI catchers
- Downgrade to 3G/2G or lower generations with unprotected messages (Registration Reject: LTE not allowed)
  - Automatic timer-based recovery? Not implemented in many phones
- Downgrading to 3G or 2G may require some sophistication (2015 vs 2021)
  - RRC release and similar messages in LTE

UE Capability exchange: protected

- Includes 4G and 5G-NR capabilities
- Vulnerability found in 2019
  - 2019 vs 2021

```
UE additional security capability
    Element ID: 0x6f
    Length: 4
    1... .... = 5G-EA0: Supported
    .1.. .... = 128-5G-EA1: Supported
    ..1. .... = 128-5G-EA2: Supported
    ...1 .... = 128-5G-EA3: Supported
    .... 0... = 5G-EA4: Not supported
    .... .0.. = 5G-EA5: Not supported
    .... ..0. = 5G-EA6: Not supported
    .... ...0 = 5G-EA7: Not supported
    0... .... = 5G-EA8: Not supported
    .0.. .... = 5G-EA9: Not supported
    ..0. .... = 5G-EA10: Not supported
    ...0 .... = 5G-EA11: Not supported
    .... 0... = 5G-EA12: Not supported
    .... .0.. = 5G-EA13: Not supported
    .... ..0. = 5G-EA14: Not supported
    .... ...0 = 5G-EA15: Not supported
    1... .... = 5G-IA0: Supported
    .1.. .... = 128-5G-IA1: Supported
    ..1. .... = 128-5G-IA2: Supported
    ...1 .... = 128-5G-IA3: Supported
    .... 0... = 5G-IA4: Not supported
    .... .0.. = 5G-IA5: Not supported
    .... ..0. = 5G-IA6: Not supported
```



SINTEF

Integrity protection for User Plane Data

- 4G tower carry control-traffic
- 5G NR tower carry data-traffic
  - Optional integrity protection for data-traffic
  - Not enabled in 4 NSA networks: Vulnerable to alter-attacks

SINTEF

5G IMSI Catchers - SA

- Attacks possible against 5G SA

Decoding SUCI

- IMSI/SUPI is encrypted -> not exposed over-the-air unless ‘null scheme’

- SUCI protects user privacy but reveals home operator name
  - MCC and MNC not encrypted (for routing purpose)
  - Similar in 4G, but in roaming situation, attacker still learn something
  - Example, identify foreign SUCIs in the particular area

SUCI

RED – Plaintext

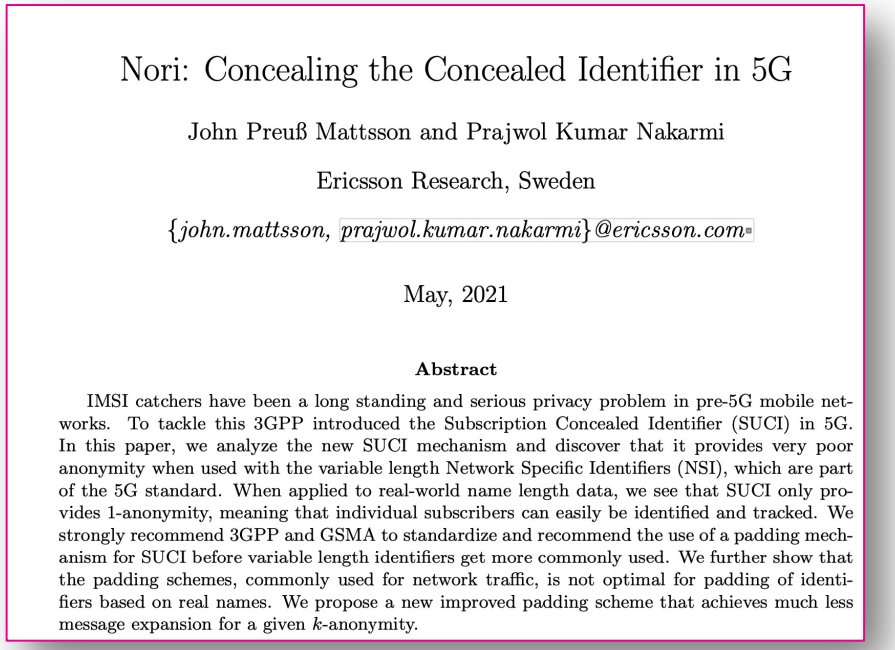
GREEN - Encrypted

SUCI
National Operator 1
National Operator 2
National Operator 3
International Operator 1 (Asia)
International Operator (Africa)

SINTEF

Decoding SUCI

- If SUPI is not based on IMSI, SUCI may not be random (lengh differs)*
  - SUPI == username@realm , for example, “bob@nsa.com”
  - Important for 5G private network deployment scenarios
  - For example, private 5G network subscribers can be easily distingushable from public 5G subscribers



Nori: Concealing the Concealed Identifier in 5G

John Preuß Mattsson and Prajwol Kumar Nakarmi

Ericsson Research, Sweden

{*john.mattsson, prajwol.kumar.nakarmi*}*@ericsson.com*

May, 2021

Abstract

IMSI catchers have been a long standing and serious privacy problem in pre-5G mobile networks. To tackle this 3GPP introduced the Subscription Concealed Identifier (SUCI) in 5G. In this paper, we analyze the new SUCI mechanism and discover that it provides very poor anonymity when used with the variable length Network Specific Identifiers (NSI), which are part of the 5G standard. When applied to real-world name length data, we see that SUCI only provides 1-anonymity, meaning that individual subscribers can easily be identified and tracked. We strongly recommend 3GPP and GSMA to standardize and recommend the use of a padding mechanism for SUCI before variable length identifiers get more commonly used. We further show that the padding schemes, commonly used for network traffic, is not optimal for padding of identifiers based on real names. We propose a new improved padding scheme that achieves much less message expansion for a given k-anonymity.

SINTEF

Tracking with 5G-AKA Vulnerabilities

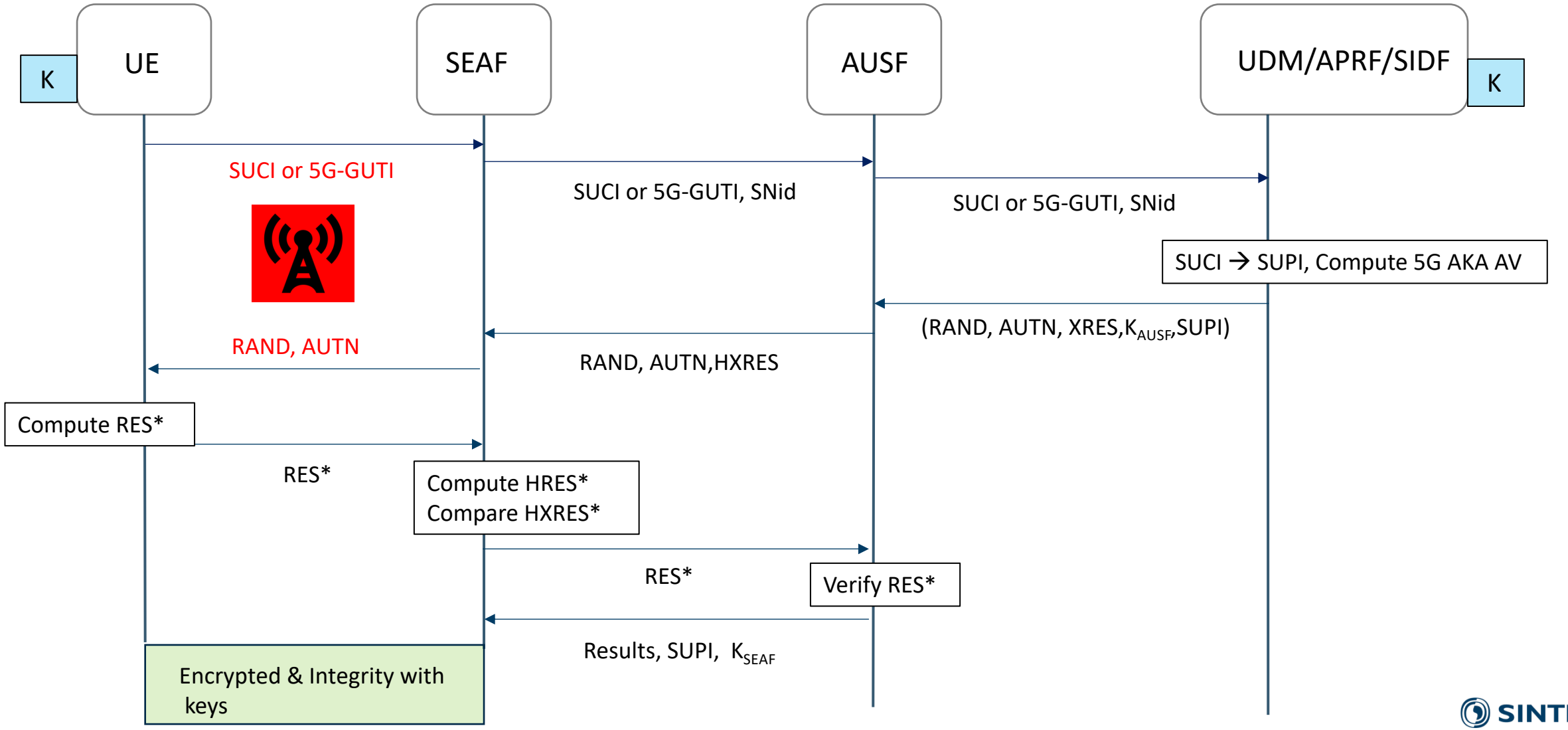
- Active type of IMSI catcher needed
- One pair of RAND, AUTN enough to identify the mobile device
  - RAND, AUTN can be sniffed or requested from the network on demand if IMSI is known (by downgrading)
- Attacker can replay RAND, AUTN with fake 5G SA base station*
- Two vulnerabilities (Our previous work in 2012**/2019***)
  - MAC or SQN failure
  - XOR in AUTS (for more details, see our PETS'18/Blackhat'19 talk)

Fig. 4. Our experimental setup, showing a smartcard reader, USRP (left), set of commercial USIM cards, and a test phone.

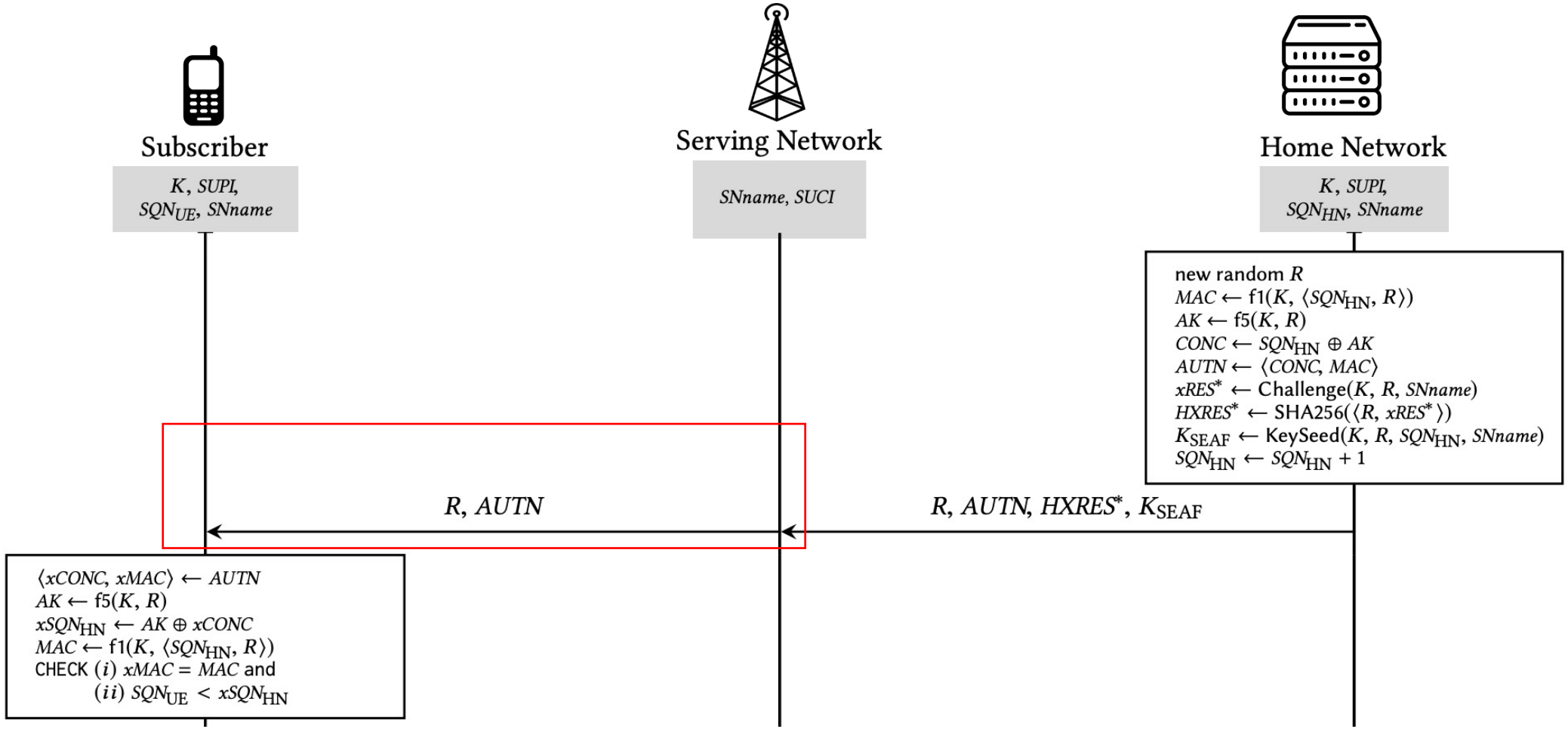
*** Ravishankar Borgaonkar, Lucca Hirschi , Shinjo Park, and Altaf Shaik New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols.
** M Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. 2012. New privacy issues in mobile telephony: fix and verification.
* Merlin Chlosta, David Rupprecht, Christina Pöpper, and Thorsten Holz. 2021. 5G SUCI-catchers: still catching them all? WiSec'21.

SINTEF

5G Authentication Protocol - AKA



5G AKA Protocol



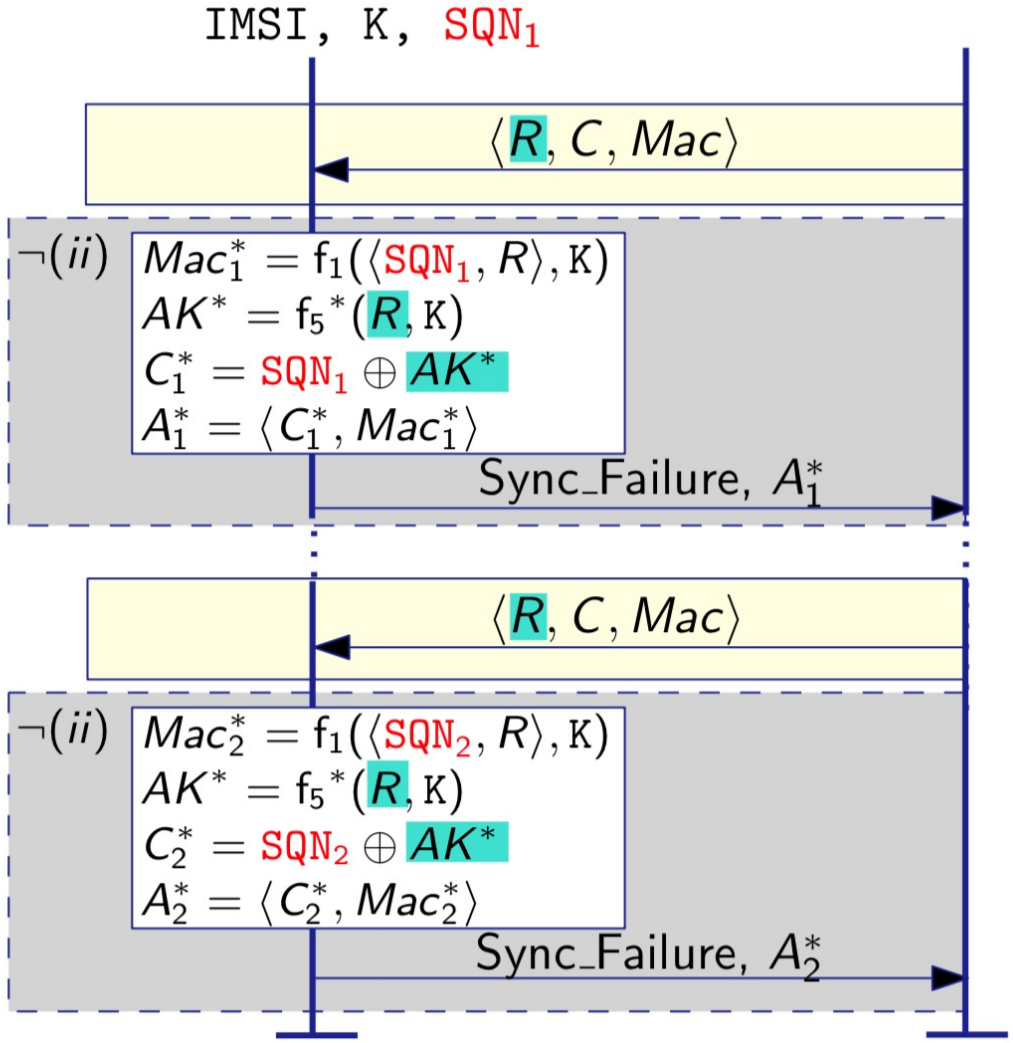
AUTN = C, MAC

SINTEF

Attack

Attack vector = combination of:

- Two injections of the same (unfresh) challenge $\rightsquigarrow$ same conceal factor AK^*
- requests of challenges are not authenticated



AUTN = C, MAC

$C_1^* \oplus C_2^* = \mathrm{SQN}_1 \oplus \mathrm{SQN}_2$

SINTEF

Downgrading to 4G

- Downgrading attack still possible from active IMSI catchers
- Downgrade to 4G or lower generations with unprotected messages (Registration Reject: 5GS not allowed)
- Downgrading to 3G or 2G may require some sophistication

Non compliance with mandatory features

Security Features	5G NSA	5G SA
Encrypted SUPI	❌	✅
Fresh 5G-GUTI reallocation	❌	✅
Paging by 5G-S-TMSI	❌	✅
ABBA parameter	❌	✅
Integrity protection	❌	✅
UE-assisted Network based IMSI catcher detection	❌	✅
Secure UE capabilities transfer	✅	✅

Wrong configuration, may allow tracking

Open issues in 5G – I

- Master-slave perspective
  - Still base station has more power in security negotiations
  - Not easy to solve due to trade-off issues though
- AKA protocol vulnerabilities
  - Though identities are encrypted, AKA protocol allows targeted tracking of mobile subscribers
- Lack of ciphering indicator for data traffic (on mobiles)
  - Standard defines ciphering indicators per PDU sessions (via API)
  - Standard does not mandate how to use APIs or ciphering indicators
  - Current smartphones does not implement or enable/enforce this feature

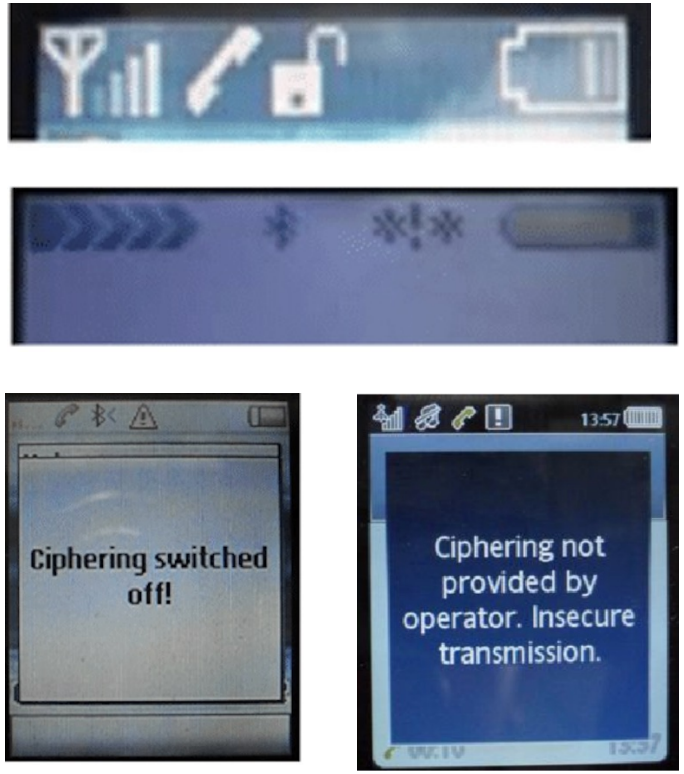


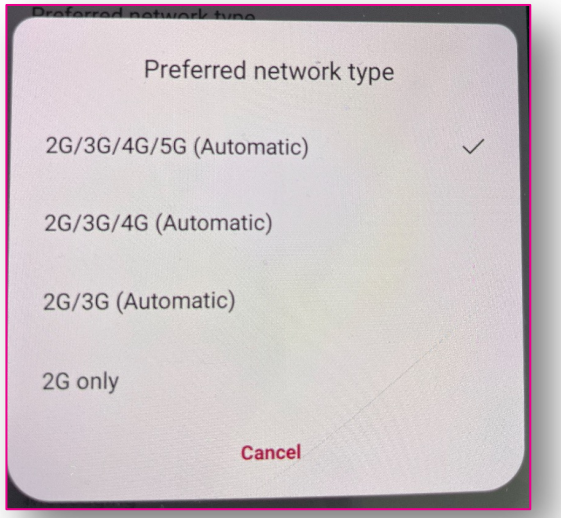
Figure Source - Iosif Androulidakis 1,*, Dionisios Pylarinos2 and Gorazd Kandus , “Ciphering Indicator approaches and user awareness”

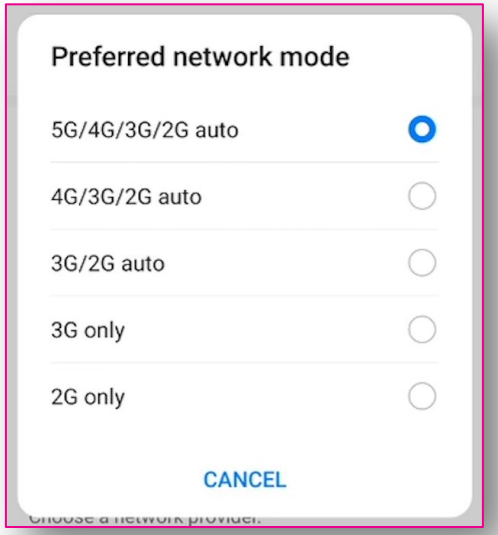
SINTEF

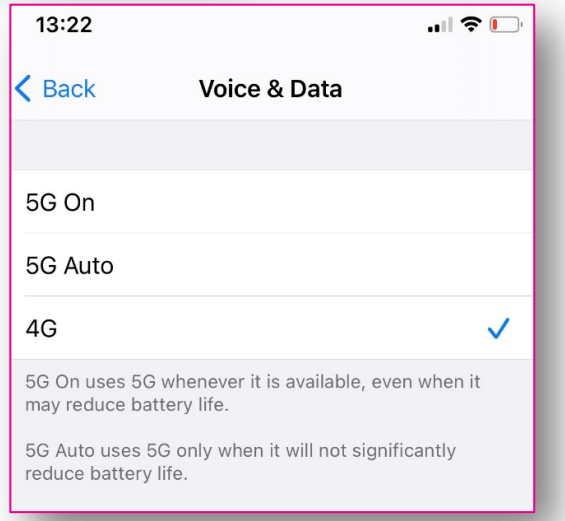
Open issues in 5G - II

- Downgrading to lower generation
  - Difficult to address considering service quality/availability
  - In future, unsecure 2G/3G networks may dissolve themselves
  - Sadly, no agility to remove from the devices

- No guidelines for OEMs for choice of secure network selection
  - 5G NSA / 5G SA mode not offered yet
  - Lack of enforcement from OEMs or operators



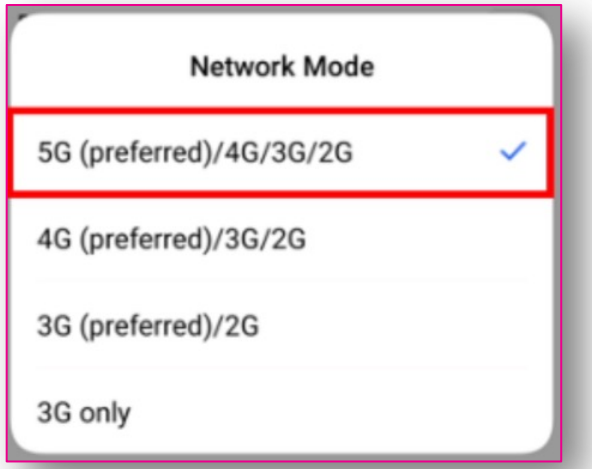




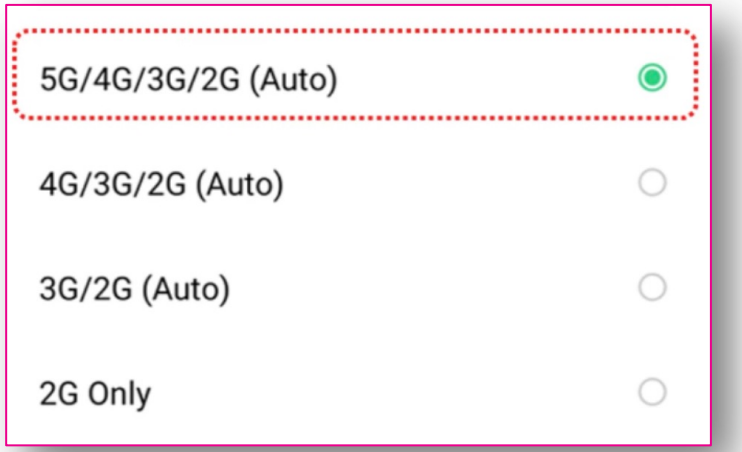
SINTEF

Open issues in 5G - III

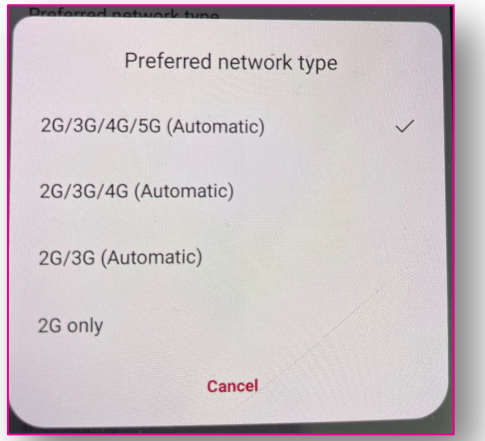
- No option for 5G only / NSA / SA only selection mode



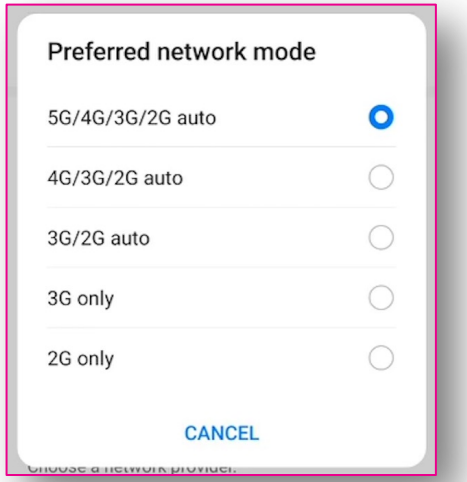
Vivo X50 Pro



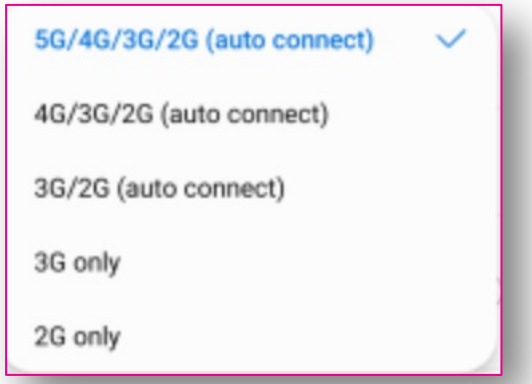
Oppo Reno 5G



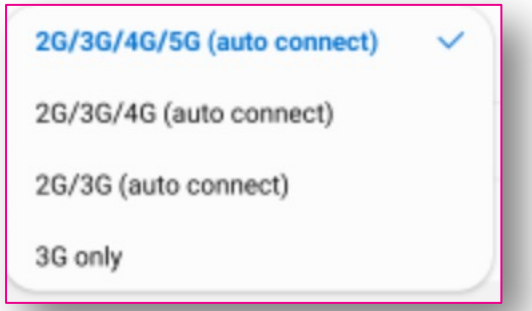
OnePlus 8T



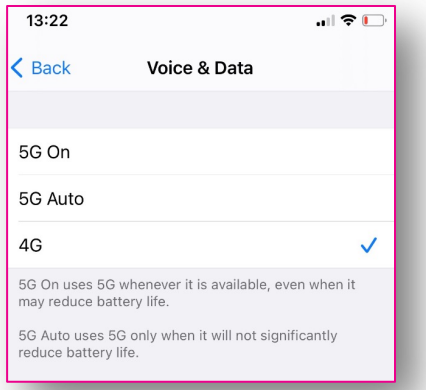
Huawei P40



Samsung S21 5G



Samsung S10 5G



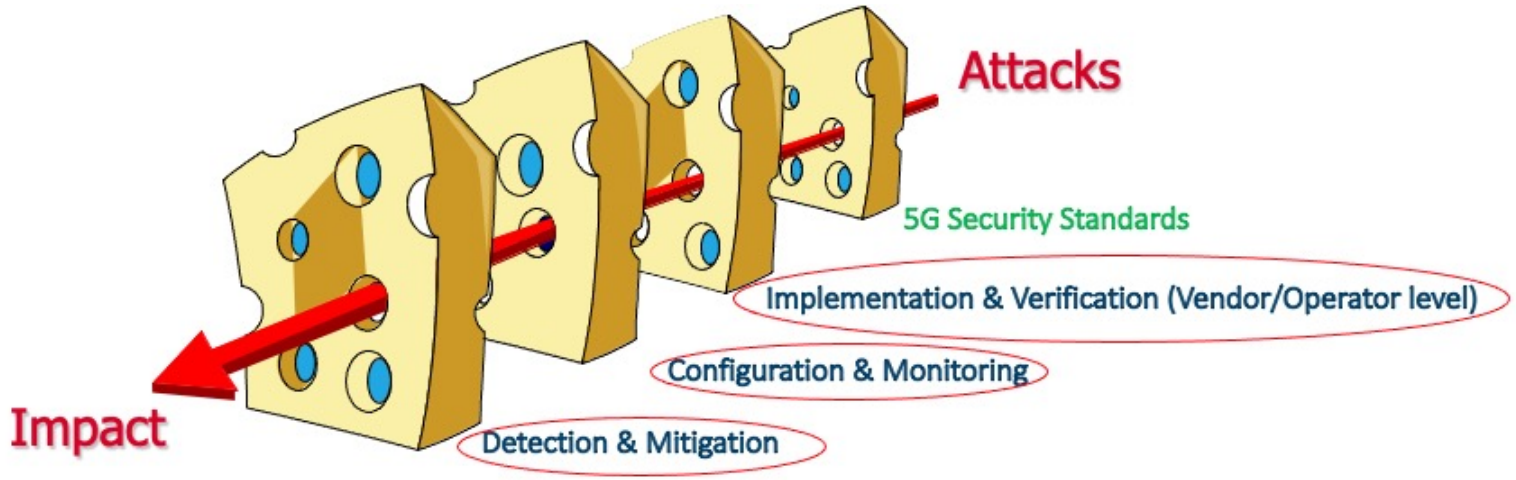
iphone 12

SINTEF

Guidelines

Operators

- GUTI freshness & randomness
- Verification of RAN features in eNB & CN
- Continuous monitoring of RAN security features (Example, some network assign all 0 for TMSI or same TMSI for 10 days)
- Mechanisms to detect IMSI catchers or bad devices (TS33.501)

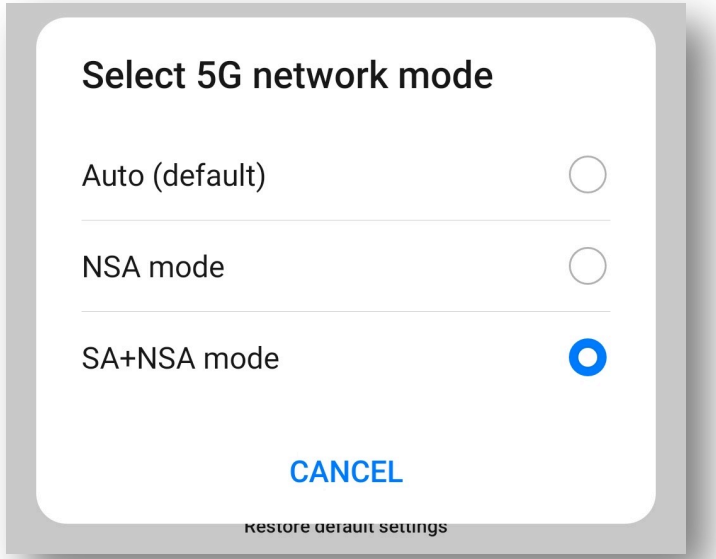


SINTEF

Guidelines

OEMs

- Verification of RAN security features
  - Example, EIA0 accepted in non-emergency calls in 4G devices- Benoit Michaue
  - IMEI leak in 4G – our work



Huawei P40 in developer mode

- Mandatory ciphering indicator for 2G/3G/4G/5G network calls

- Options to choose 5G NSA/ 5G SA / 4G only mode for users

SINTEF

Take Aways

- RAN security is improved in 5G
  - Post deployment security differs from mandatory (baseline)
- IMSI catcher attack is possible in both 5G NSA and SA networks!
  - 4G RAN security == 5G NSA **(false sense of 5G security)**
  - Unfixed radio protocols (AKA & attach protocols still allows targeted attacks)
  - SUCI decoding enables identification of roaming subscribers
  - For end users, no control over choosing the most secure network
  - No security indicators for connected network either call or data traffic
- Lack of enforcement of security features in operational networks allow tracking of 5G users easily
  - Need continuous & proactive security monitoring of 5G RAN configurations

Thank You.

Teknologi for et bedre samfunn

Acknowledgement

This work is funded by Raksha: 5G Security for Critical Communications (312122), a four-year project funded under the “IKTPLUSS-IKT og Digital Innovasjon” programme. The authors gratefully acknowledge the financial support from the Research Council of Norway.