Privacy of subscribers in mobile networks: *changes and challenges over time*

Ruxandra F. Olimid

University of Bucharest, Romania

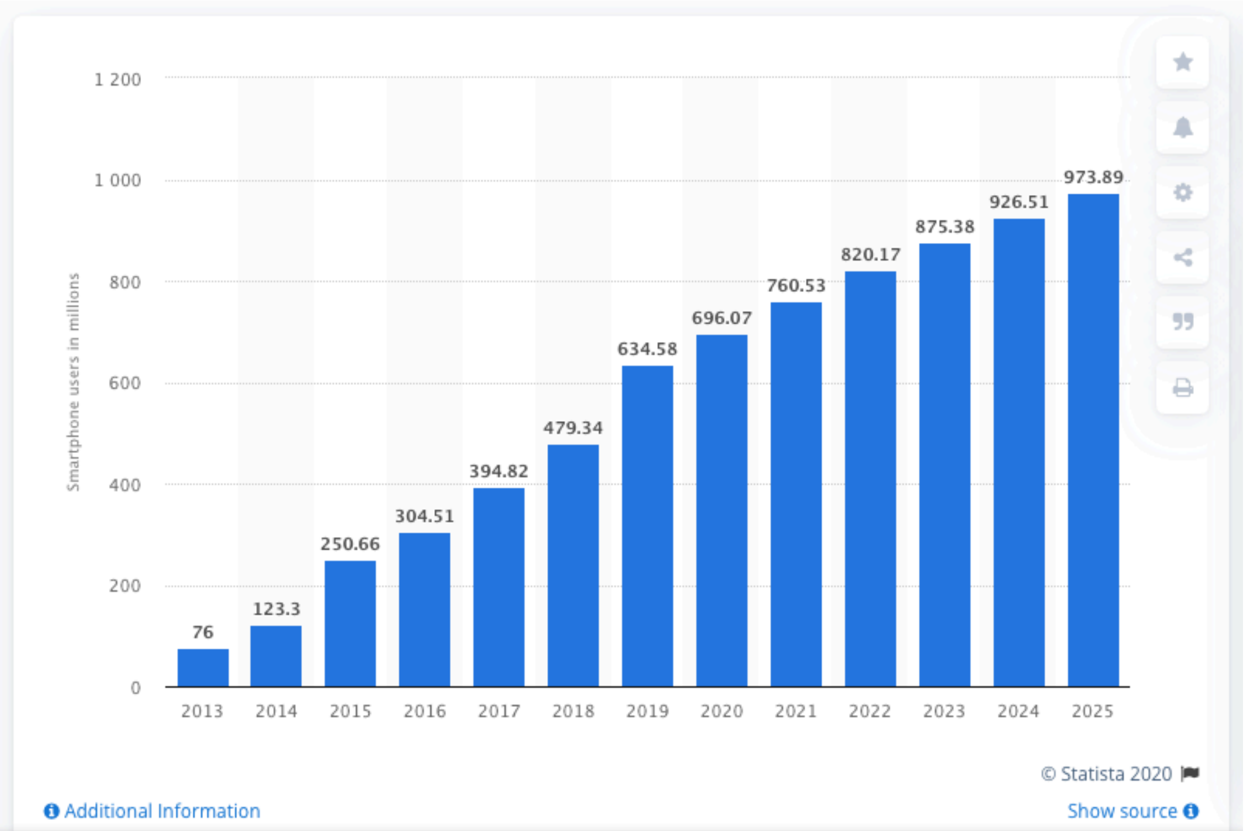
Norwegian University of Science and Technology - NTNU, Norway

October 17th, 2020

Webinar on Cryptography, Network Security and Cybersecurity

Motivation

[Source: https://www.statista.com/statistics/467163/forecast-of-smartphone-users-in-india/]



Estimated human population:
7.8 billions (oct.2020)

Smartphone users in India 2015-2025

Published by Vaibhav Asher, Sep 10, 2020

The number of smartphone users in India was estimated to reach over 760 million in 2021, with the number of smartphone users worldwide forecasted to exceed to 3.8 billion users in 2021.

Mobile Networks Evolution

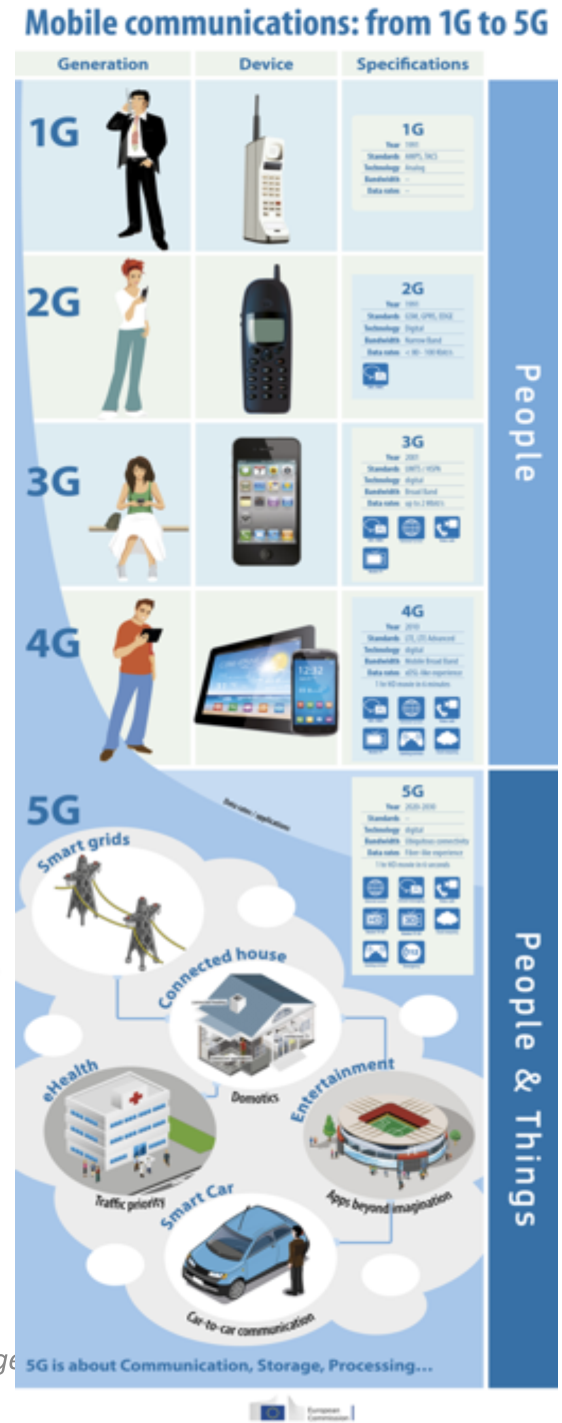
mechanisms

vulnerabilities

ideas

2G → 3G → 4G → 5G

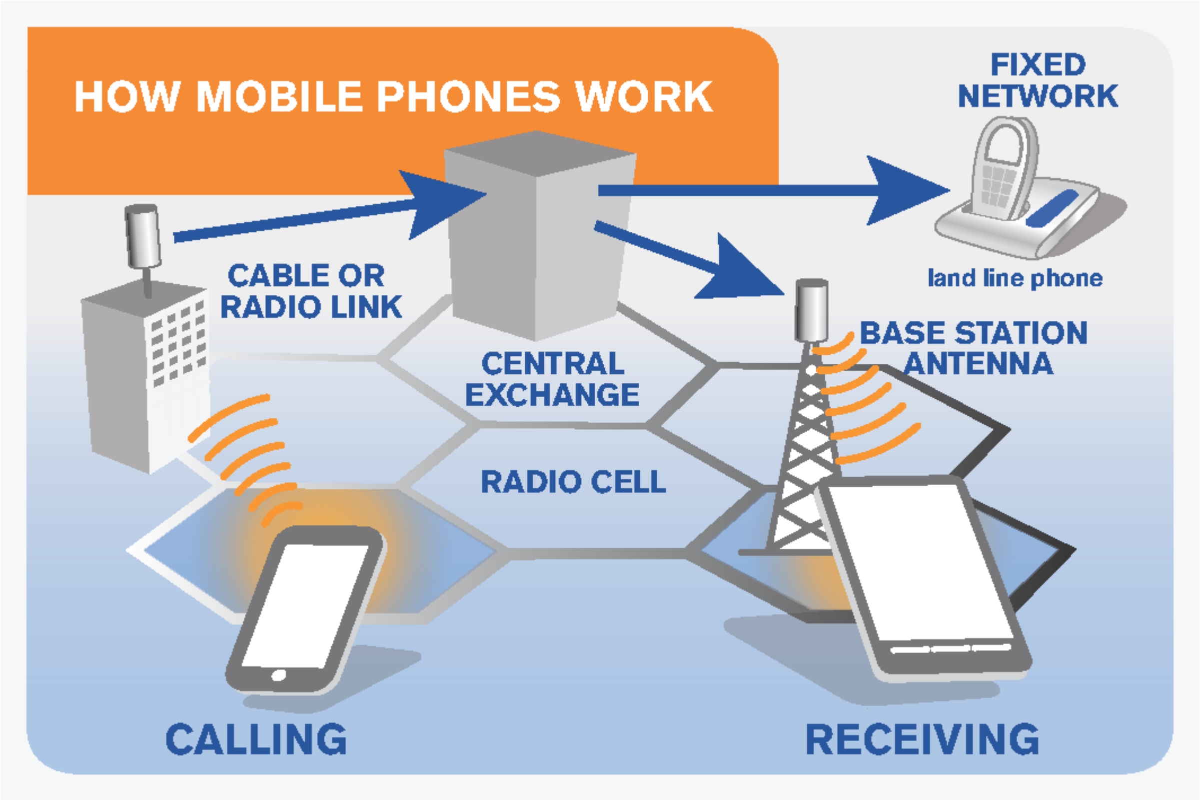
Security improvements →



[Source: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_129]

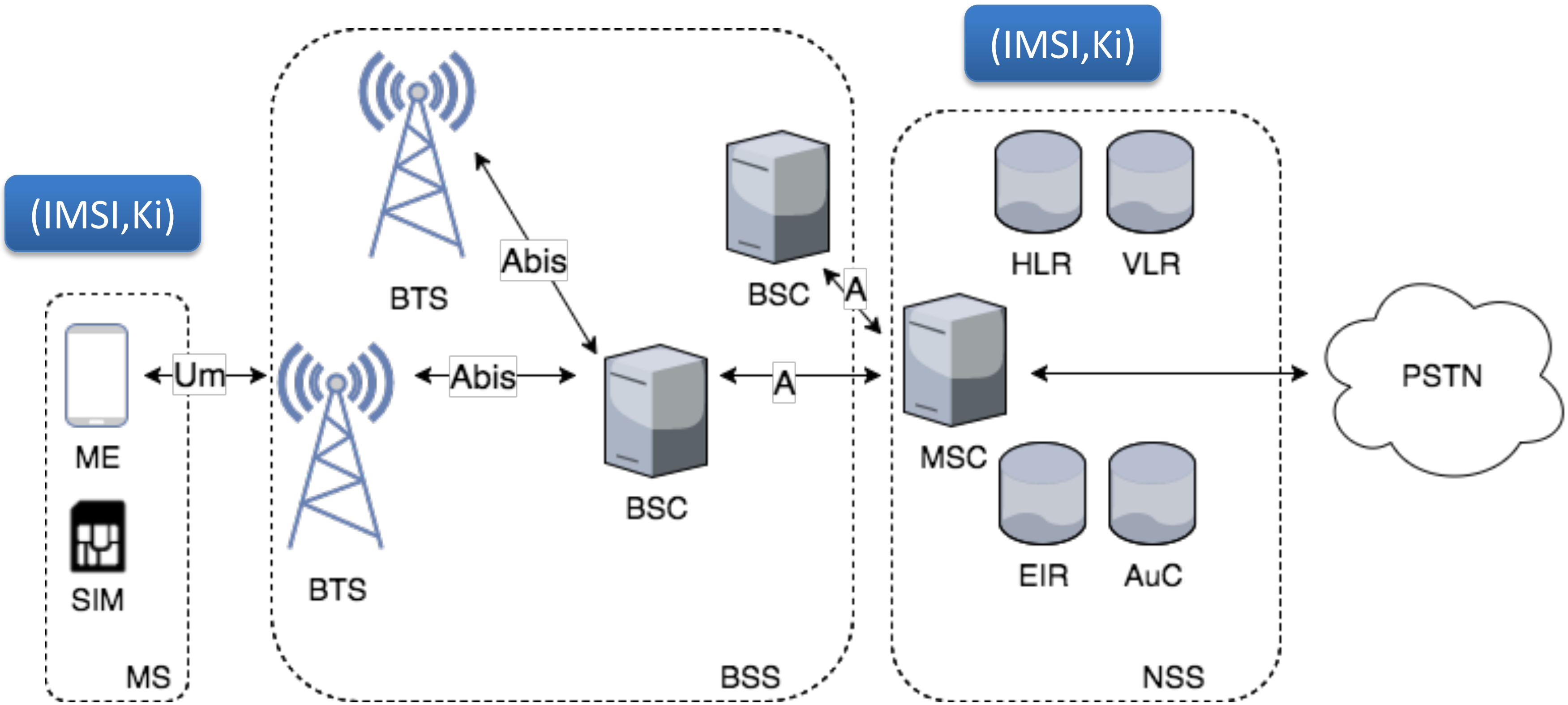
Mobile Networks General Architecture

- User equipment
- Access network
  - Radio link
- Core network



[Source: http://emfguide.itu.int/emfguide.html]

The Global System for Mobile Communications (GSM)



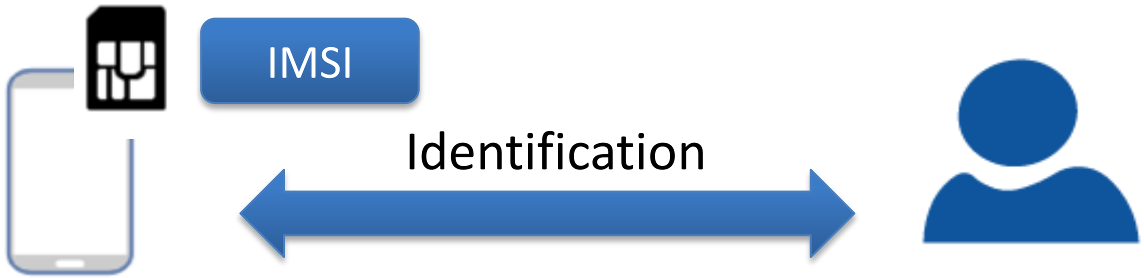
MS: Mobile Station
ME: Mobile Equipment
SIM: Subscriber Identity Module

BSS: Base Station Subsystem
BTS: Base Transceiver Station
BSC: Base Station Controller

NSS: Network Subsystem
MSC: Mobile Services Switching Center
HLR: Home Location Register
VLR: Visitor Location Register
EIR: Equipment Identity Register
AuC: Authentication Center

PSTN: Public Switched Telephone Network

Identification of Subscribers

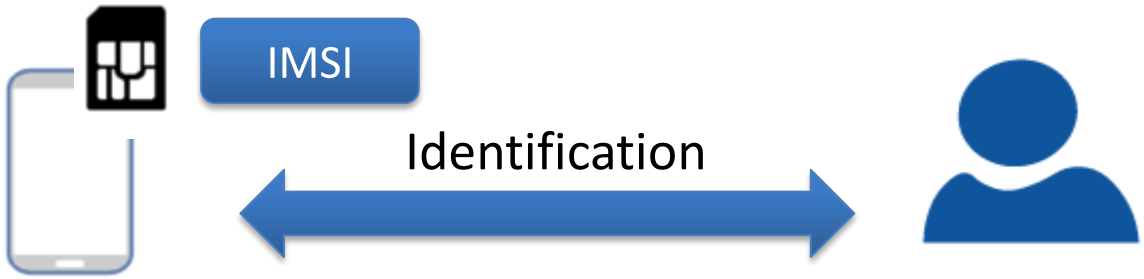


IMSI (International Mobile Subscriber Identity)

MCC (Mobile Country Code) - 3 digits -	**MNC** (Mobile Network Code) - 2 digits (EU) / 3 digits (US) -	**MSIN** (Mobile Subscriber Identification Number)
404,405 (India)	81 (BSNL) / 44 (Spice)	XXXXXXXXXX
242 (Norway)	01 (Telenor) / 02 (Telia)	XXXXXXXXXX
226 (Romania)	01 (Vodafone) / 10 (Orange)	XXXXXXXXXX

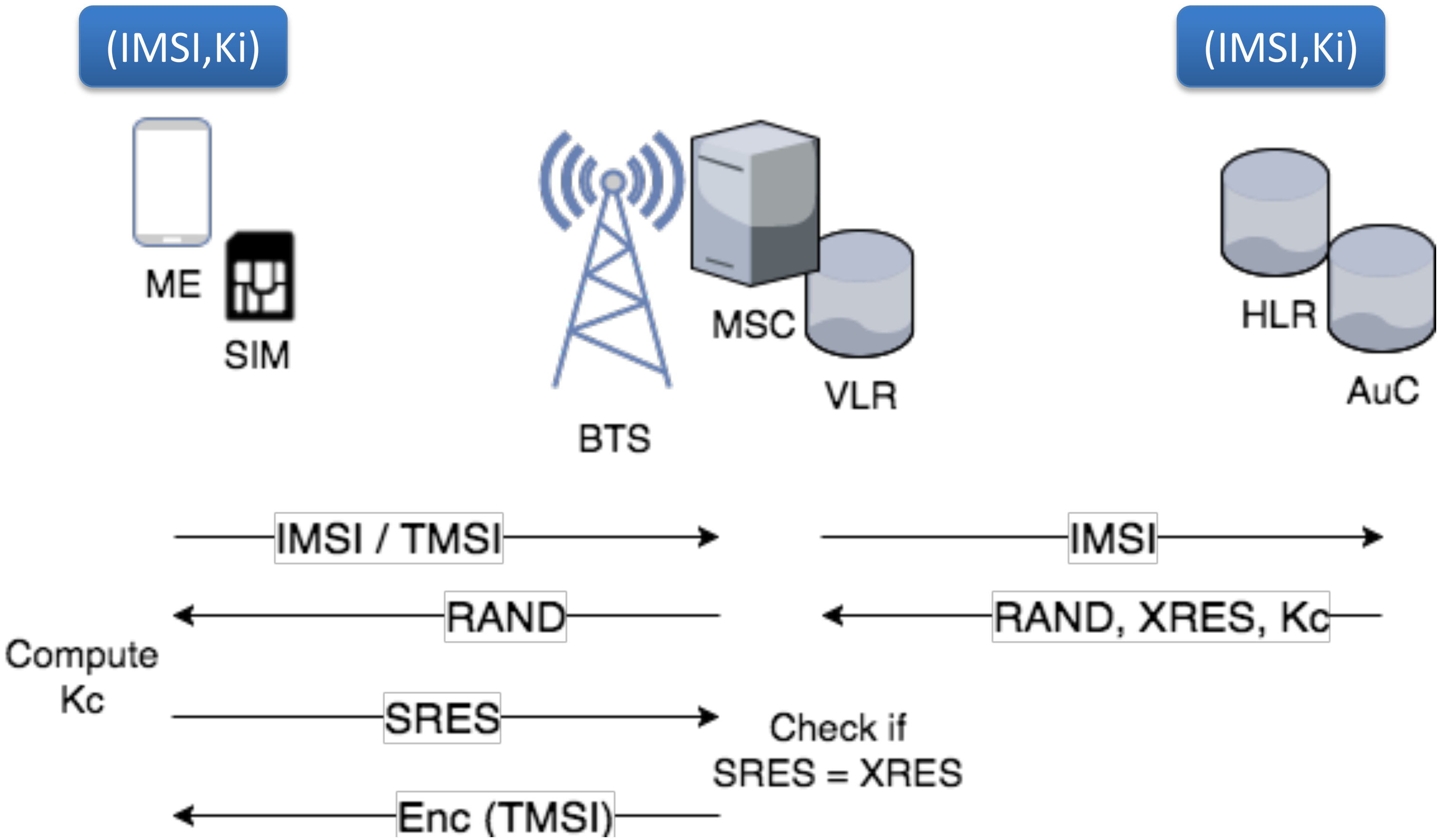
[List of MCCs and MNCs: http://mcc-mnc.com/]

Identification of Subscribers



- **IMSI** (International Mobile Subscriber Identity)
- **TMSI** (Temporary Mobile Subscriber Identity)
- **Ki** (cryptographic key)

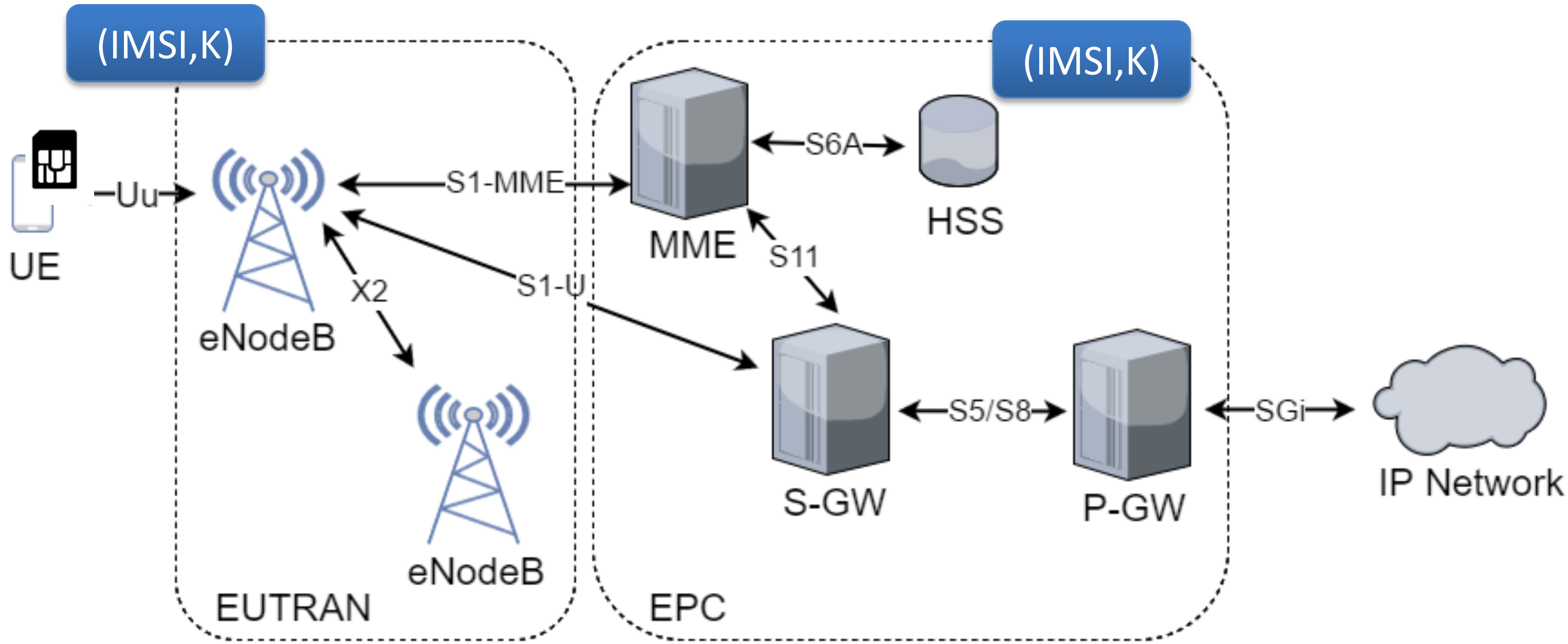
Authentication of Subscribers (GSM)



$Kc = A8(K_i, RAND)$

$SRES / XRES = A3(K_i, RAND)$

Long Term Evolution (LTE)



UE: User Equipment
USIM: Universal Subscriber Identity Module

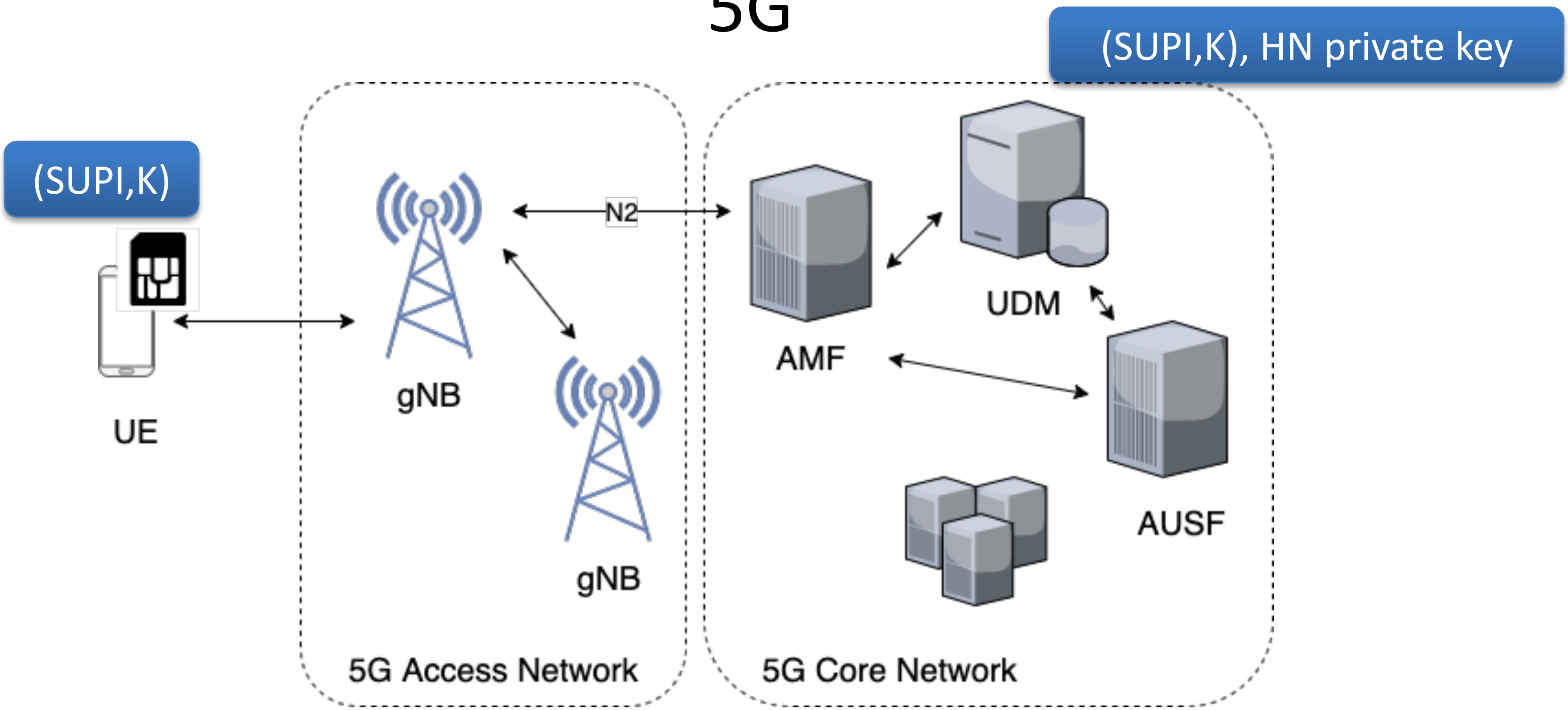
EUTRAN: Evolved UTRAN
EPC: Evolved Packet Core
eNodeB: Evolved NodeB

MME: Mobility Management Entity
S-GW: Serving Gateway
P-GW: PDN-Gateway
HSS: Home Subscriber Server

IMSI (International Mobile Subscriber Identity)

MCC (Mobile Country Code)	**MNC** (Mobile Network Code)	**MSIN** (Mobile Subscriber Identification Number)

5G



UE: User Equipment
USIM: Universal Subscriber Identity Module

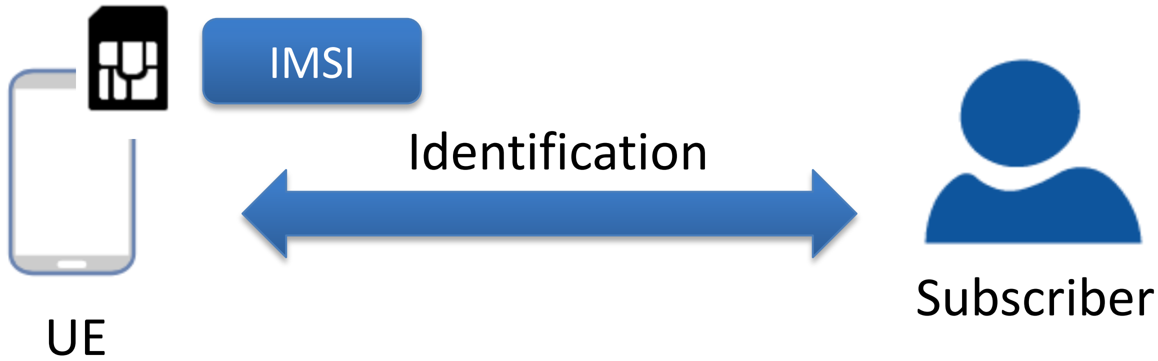
gNB: Next Generation NodeB

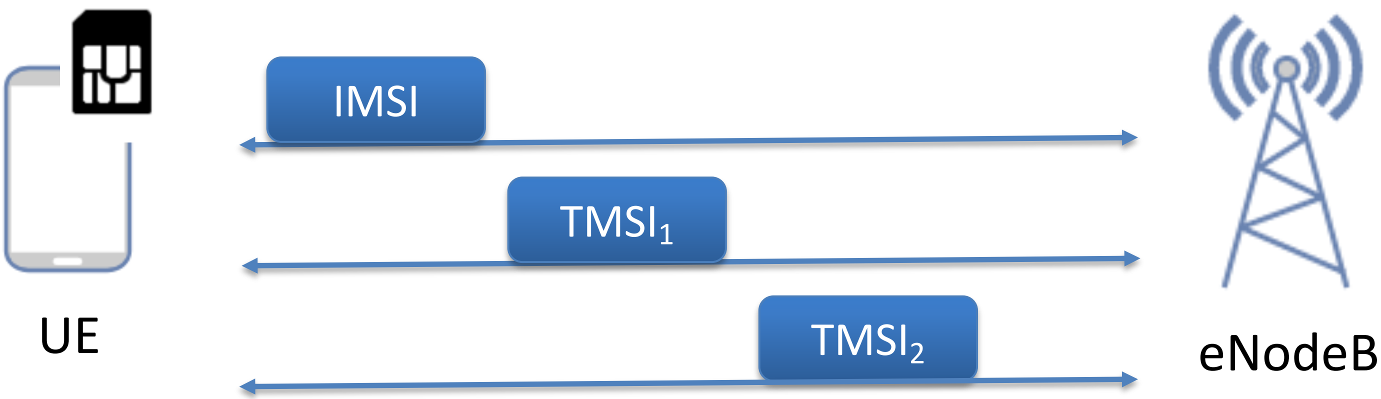
AMF: Access and Mobility Management Function
AUSF: Authentication Server Function
UDM: Unified Data Management

SUPI (Subscription Permanent Identifier)

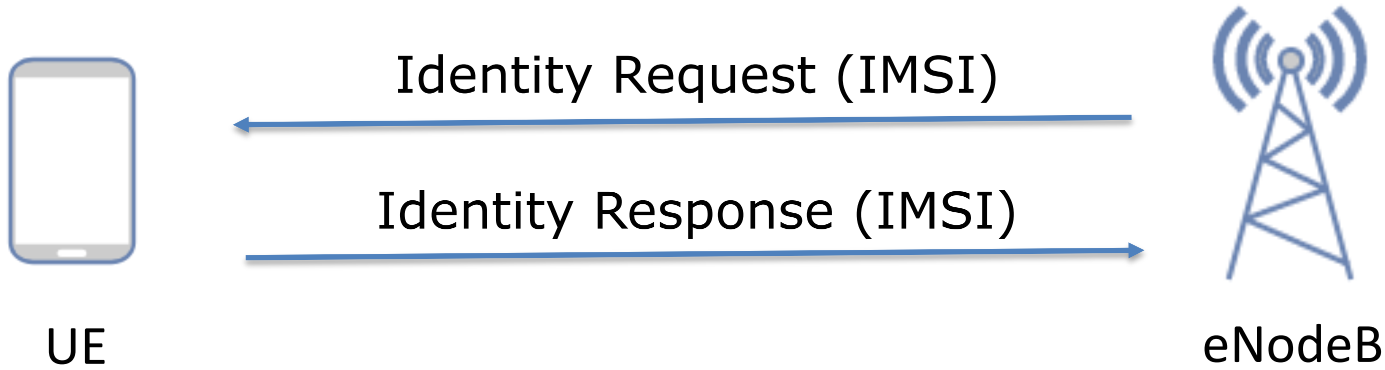
IMSI (International Mobile Subscriber Identity)	or	**NAI** (Network Access Identifier)

The Role of the TMSI





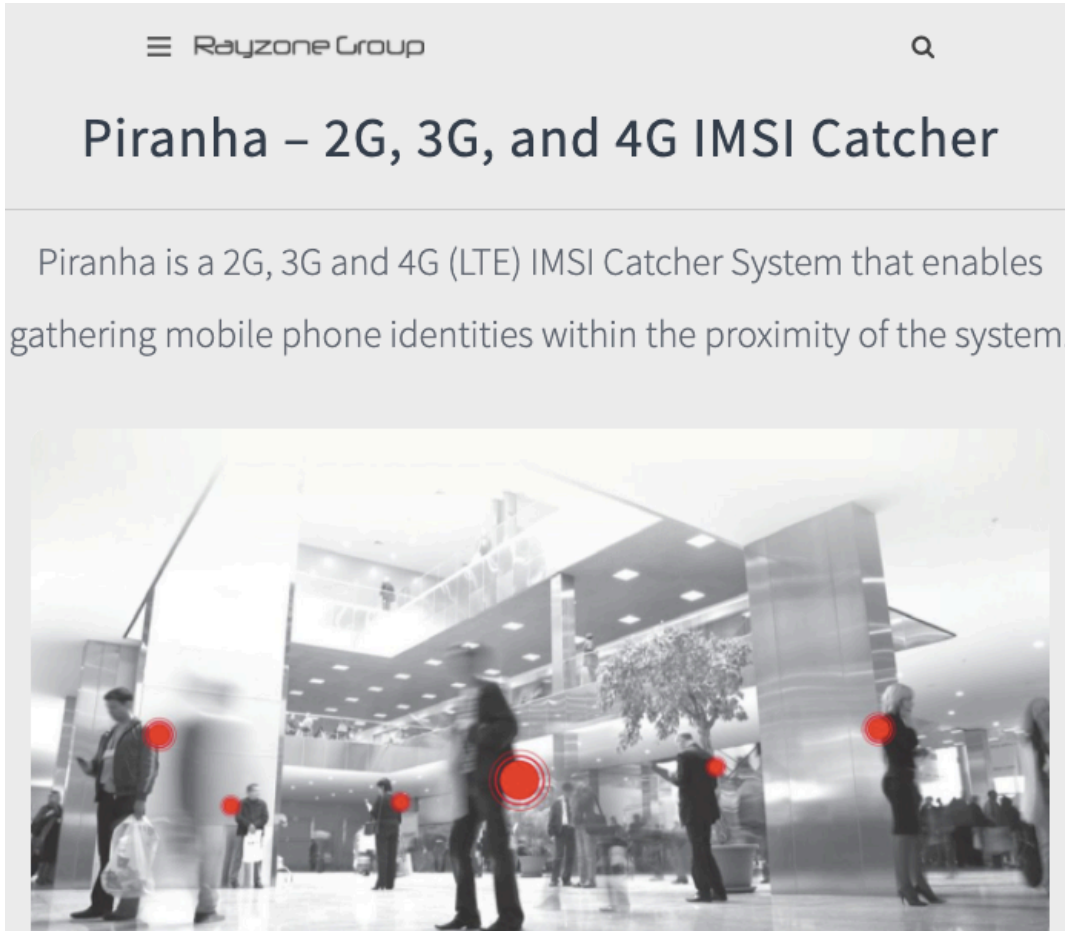
Assumed Privacy Breach



*"The mechanism is initiated by the MME that requests the user to send its permanent identity. The user's response contains the IMSI in cleartext. This represents **a breach in the provision of user identity confidentiality.**"*

[3GPP TS 33.401 V16.3.0 (2020-07)]

IMSI Catchers in the real world



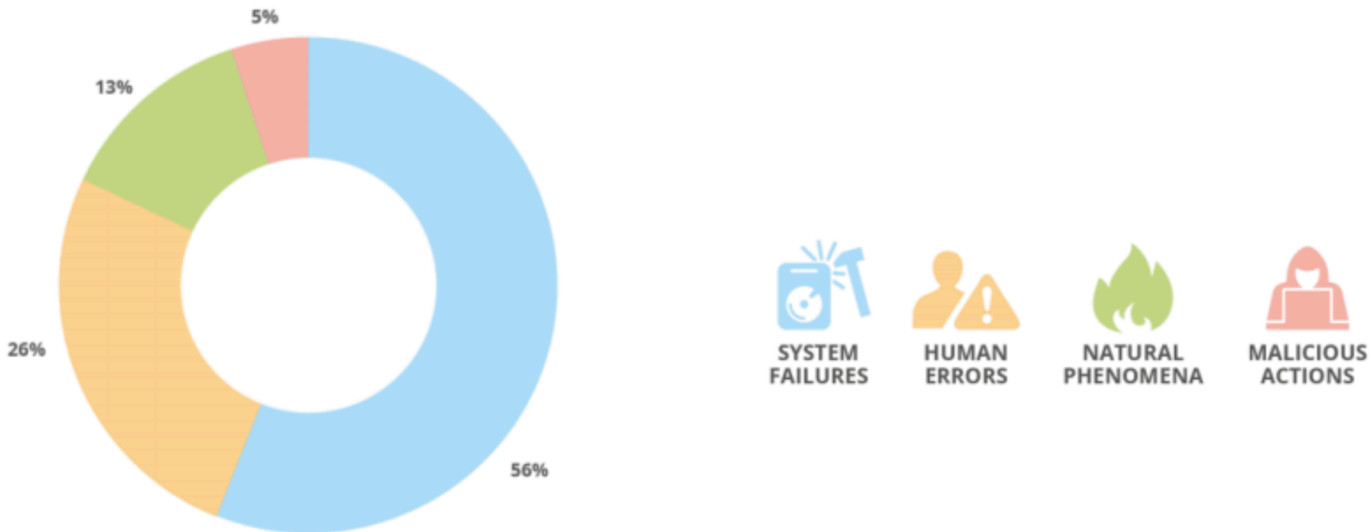
[Source: https://rayzone.com/products/piranha-2g-3g-and-4g-imsi-catcher/]

Attacks in the real world

3.1 ROOT CAUSE CATEGORIES

In 2019 more than half of the telecom security incidents were system failures. This is consistent with previous years, although somewhat lower. Often they are hardware failures and software bugs. Human errors show an increase, rising up to one fourth of the security incidents. Most often these are accidental cable cuts and faulty software changes/updates. 13% of the incidents are caused by natural phenomena also increased up to 30% compared to the previous year. Only 5% of incidents were due to malicious actions. Typically these cases are denial of service attacks, cable theft and arson.

Figure 6: Root cause categories Telecom security incidents – 2019



[Source: https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2019]

Evolution in time

2G 3G 4G

Security improvements

Increased technical capabilities at large scale

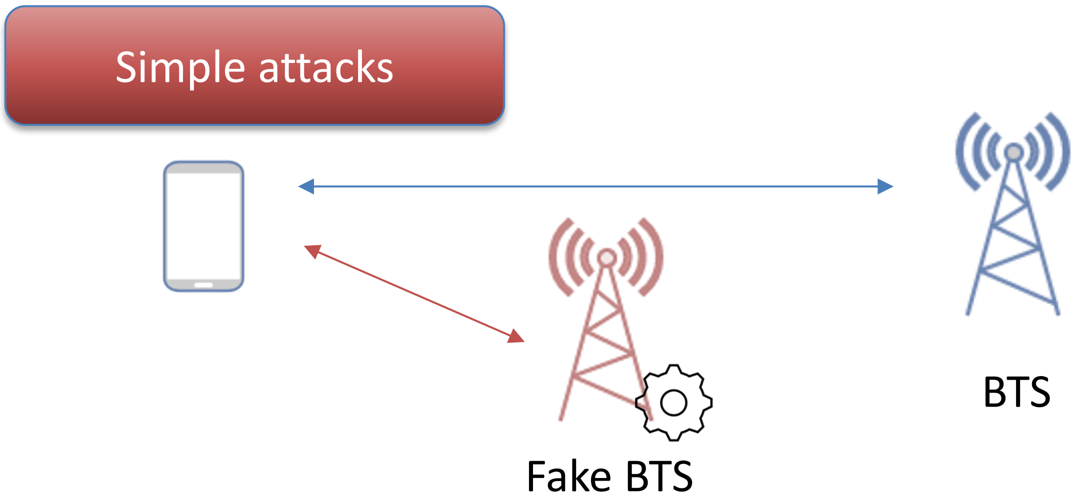
Simpler attacks

More difficult to obtain the tools

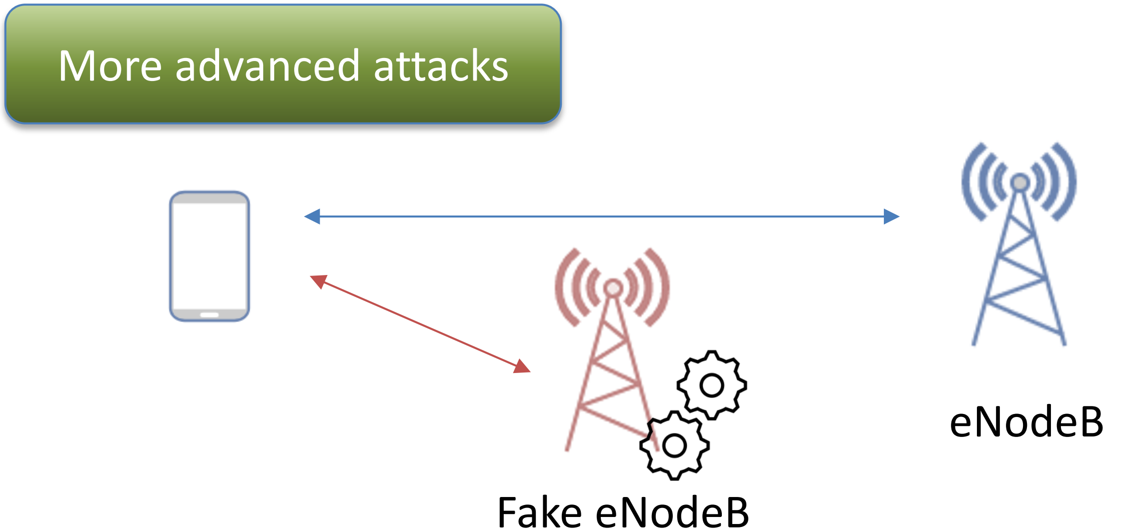
More advanced attacks

Easiest to obtain the tools

Difficulty of attacks



- Location
- Basic config.



- Location
- More advanced config. (e.g., priorities, thresholds)

Availability of low-cost tools at large scale

Easy to obtain the tools

Facilitates attacks

Easy to obtain the tools

Facilitates experimentation

OPEN AIR INTERFACE

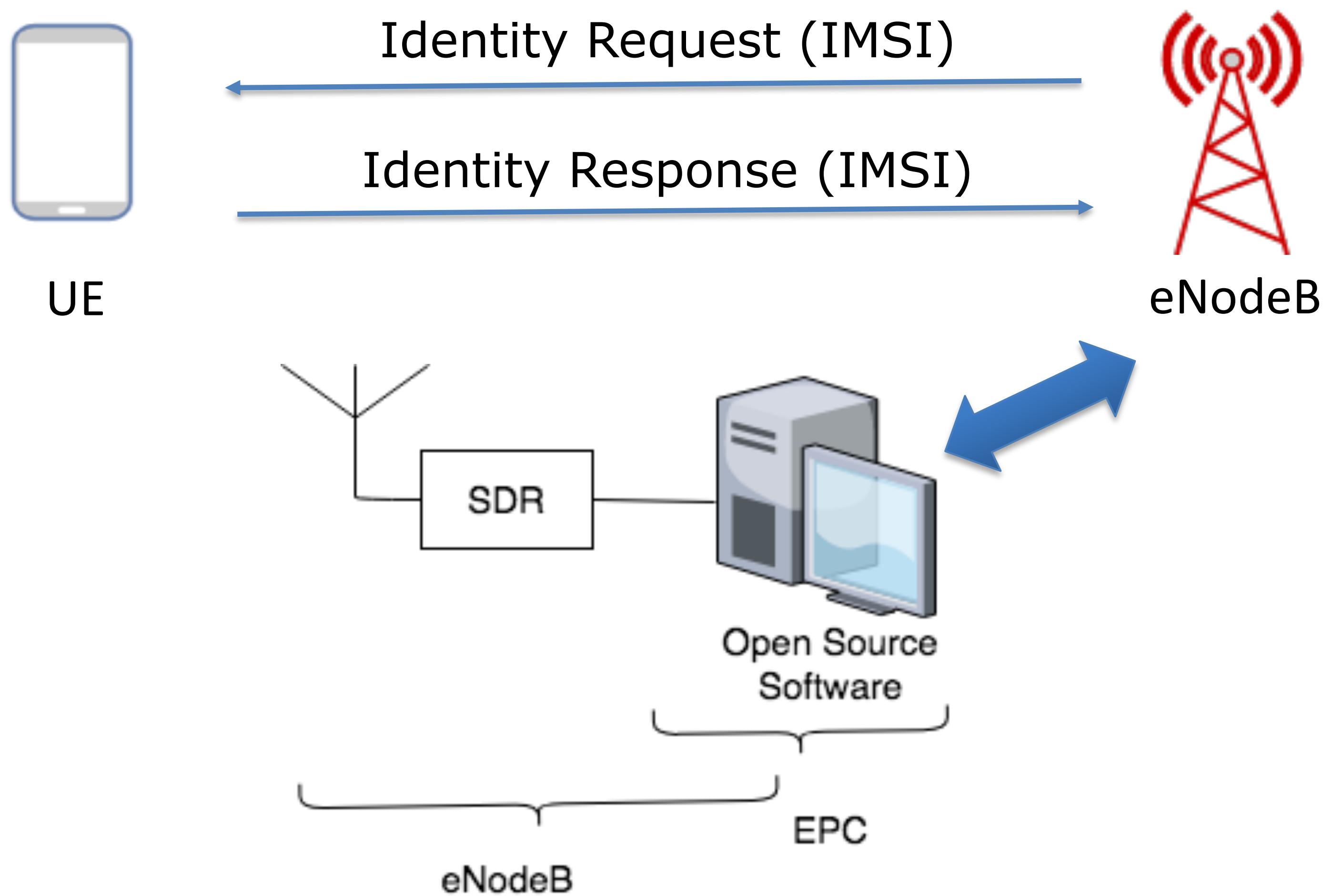
SRS SOFTWARE RADIO SYSTEMS

OpenBTS.ORG

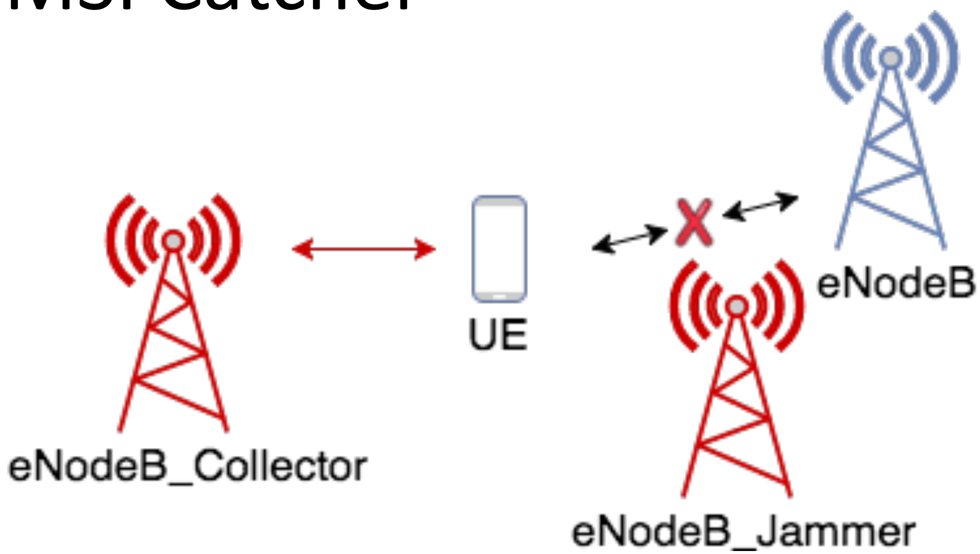
HackRF One

Ettus B200mini

Experimental Work



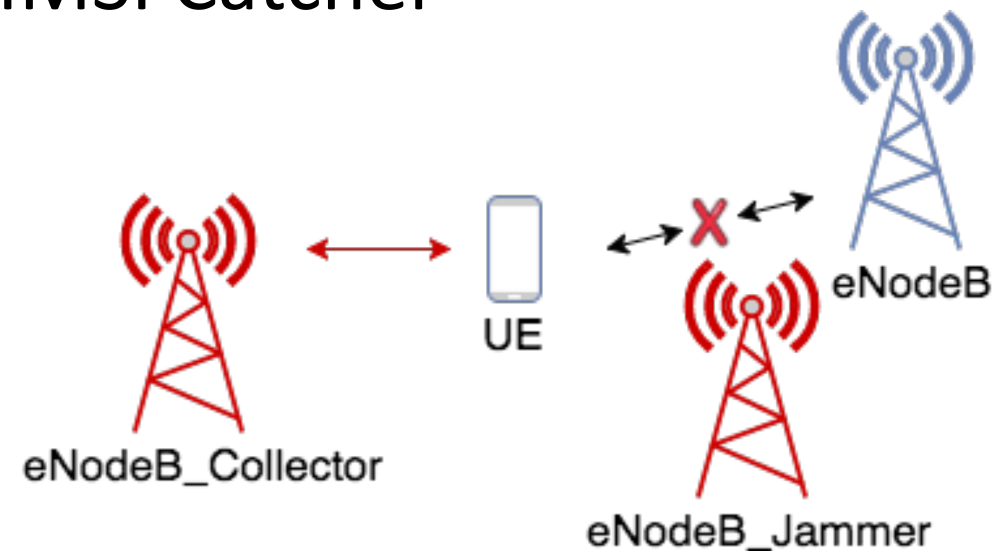
Our IMSI Catcher



- `eNodeB_Jammer:` causes the UE to detach from the serving cell it camps on
- `eNodeB_Collector:` masquerades as an authorized eNodeB running on the (second) highest **priority frequency**, but with higher signal power, causing the UE to try reselection and expose the IMSI

Mjølsnes, S.F. and Olimid, R.F., MMM-ACNS 2017, *Easy 4G/LTE IMSI catchers for non-programmers*

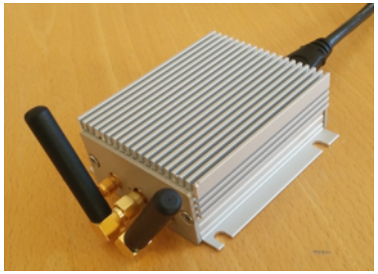
Our IMSI Catcher



- **Phase 1. Gather the configuration parameters:**
  - Find the EARFCN DL and TAC (using the Samsung device)
  - Run `eNodeB_Jammer` using MCC, MNC and the EARFCN DL of the commercial cell
  - Read new EARFCN DL after reselection
- **Phase 2. Configure and run the LTE IMSI Catcher:**
  - Run `eNodeB_Collector` using MCC, MNC and the new EARFCN DL after reselection in the commercial network, but a different TAC
  - Run `eNodeB_Jammer` configured as in Phase 1

Mjølsnes, S.F. and Olimid, R.F., MMM-ACNS 2017, *Easy 4G/LTE IMSI catchers for non-programmers*

Our IMSI Catcher: Hardware



- Software radio peripherals (USRPs)
  - Ettus B200mini + antennas
- Computers (access and core network)
  - Standard desktops or laptops: Intel NUC D54250WYK (i5-4250U CPU@1,30GHz), Lenovo ThinkPad T460s (i7-6600U CPU@2,30GHz)

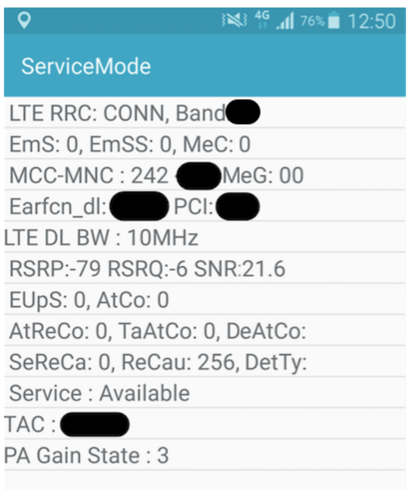
[https://www.ettus.com/product/details/USRP-B200mini]

- Mobile terminals:
  - Samsung Galaxy S4 device, used to find the LTE channels and TACs used in the targeted area
  - Two LG Nexus 5X phones running Android v6, used to test our IMSI Catcher
- SIM cards

Mjølsnes, S.F. and Olimid, R.F., MMM-ACNS 2017, *Easy 4G/LTE IMSI catchers for non-programmers*

Our IMSI Catcher: Software

- LTE Emulator:
  - **Open Air Interface (OAI),** an open source software that provides a (partially) standard compliant implementation of LTE



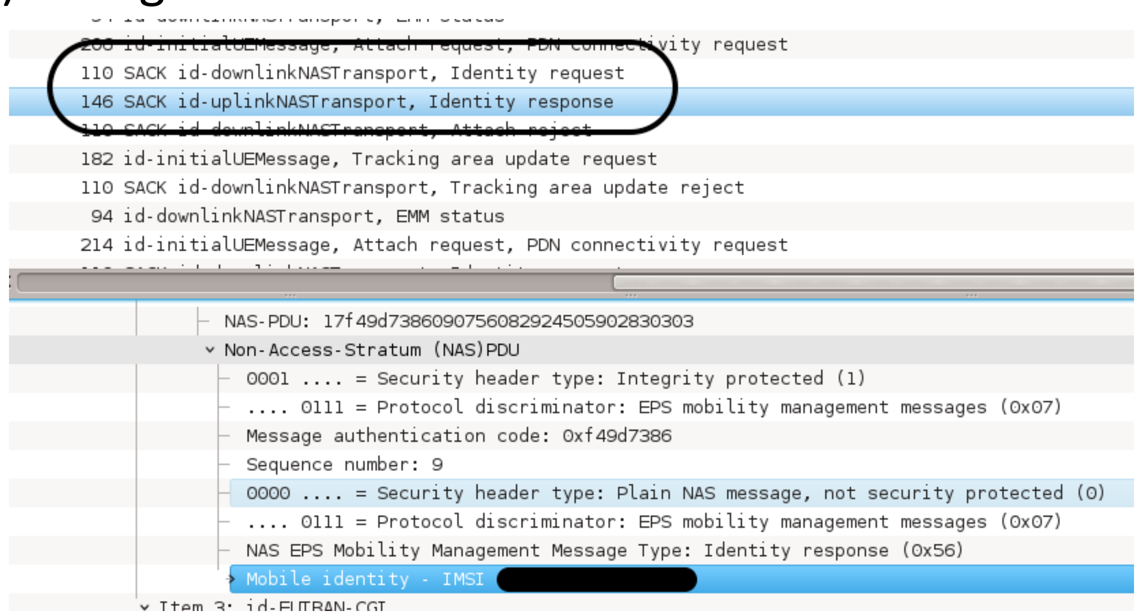
Service Mode:
- Dial *#0011# on Samsung Galaxy S4 device
- Read configuration of the commercial network: EARFCN DL, TAC, MCC, MNC, Cell ID

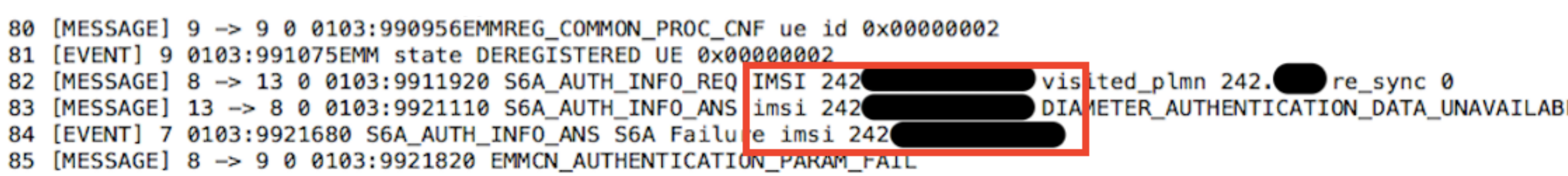
Mjølsnes, S.F. and Olimid, R.F.,MMM-ACNS 2017, *Easy 4G/LTE IMSI catchers for non-programmers*

Our IMSI Catcher: **Results**

Mjølsnes, S.F. and Olimid, R.F.,MMM-ACNS 2017, *Easy 4G/LTE IMSI catchers for non-programmers*

- Low-cost IMSI Catcher (< 3000 EUR):
  - COTS hardware and readily available software only
  - No (or very basic) changes in the source code



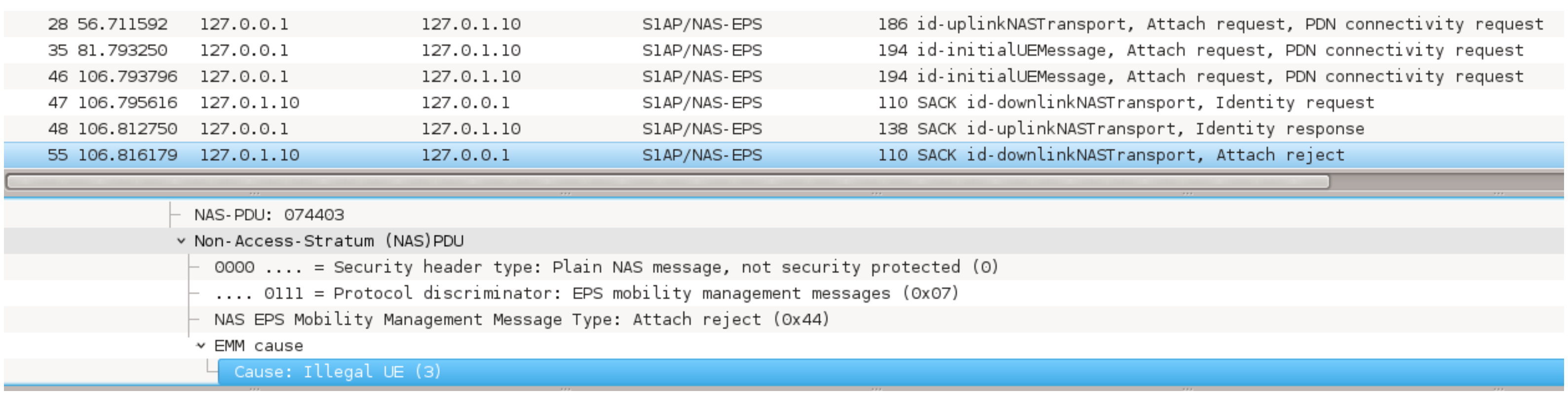


-ACNS

Our IMSI Catcher: **Results**

Mjølsnes, S.F. and Olimid, R.F., SECRYPT 2017. *Experimental Assessment of Private Information Disclosure in LTE Mobile Networks*.

- Behaviour:
  - Denial-of-Service (DoS) until reboot - *cause 3* (`Illegal UE`)
  - Downgrade to non-LTE services - *cause 7* (`EPS services not allowed`)
  - Reconnection to the commercial network - *cause 15* (`No suitable cells in tracking area`)



Many Publications and Results

Google Scholar | IMSI catcher

Articles — About 1,840 results (**0.05** sec)

Any time
Since 2020
Since 2019
Since 2016
Custom range...

Sort by relevance
Sort by date

☑ include patents
☑ include citations

Create alert

[PDF] **IMSI catcher** — [PDF] psu.edu
D Strobel - Chair for Communication Security, Ruhr-Universität …, 2007 - Citeseer
On July 29, 2005, Osman Hussain was arrested in an apartment in Rome, suspected of having placed a bomb on July 21 in a London tube station. The British Police had provided the Italian counterparts with two mobile numbers linked to him. Within 48 hours, his location …
Cited by 77 Related articles All 4 versions

IMSI-catch me if you can: **IMSI-catcher-catchers** — [PDF] acm.org
A Dabrowski, N Pianta, T Klepp, M Mulazzani… - Proceedings of the 30th …, 2014 - dl.acm.org
ABSTRACT **IMSI Catchers** are used in mobile networks to identify and eavesdrop on phones. When, the number of vendors increased and prices dropped, the device became available to much larger audiences. Self-made devices based on open source software are …
Cited by 90 Related articles All 14 versions

Easy 4G/LTE **IMSI catchers** for non-programmers — [PDF] arxiv.org
SF Mjølsnes, RF Olimid - … Models, and Architectures for Computer Network …, 2017 - Springer
IMSI Catchers are tracking devices that break the privacy of the subscribers of mobile access networks, with disruptive effects to both the communication services and the trust and credibility of mobile network operators. Recently, we verified that **IMSI Catcher** attacks are …
Cited by 28 Related articles All 7 versions

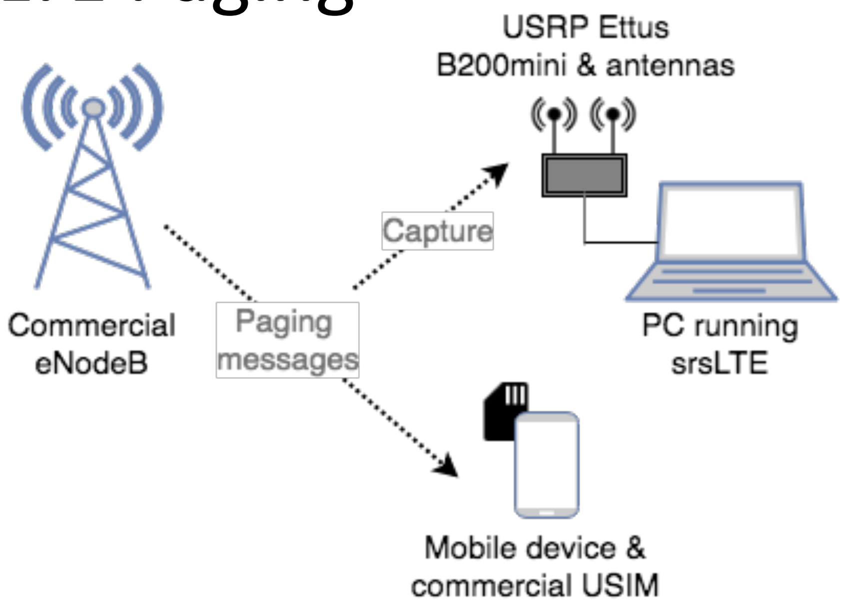
Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems

Altaf Shaik*, Ravishankar Borgaonkar[†], N. Asokan[‡], Valtteri Niemi[§] and Jean-Pierre Seifert*
*Technische Universität Berlin and Telekom Innovation Laboratories
Email: (altaf329, jpseifert) @sec.t-labs.tu-berlin.de
[†]Aalto University
Email: ravishankar.borgaonkar@aalto.fi
[‡]Aalto University and University of Helsinki
Email: asokan@acm.org
[§]University of Helsinki
Email: valtteri.niemi@helsinki.fi

LTE security, protocol exploits and location tracking experimentation with low-cost software radio

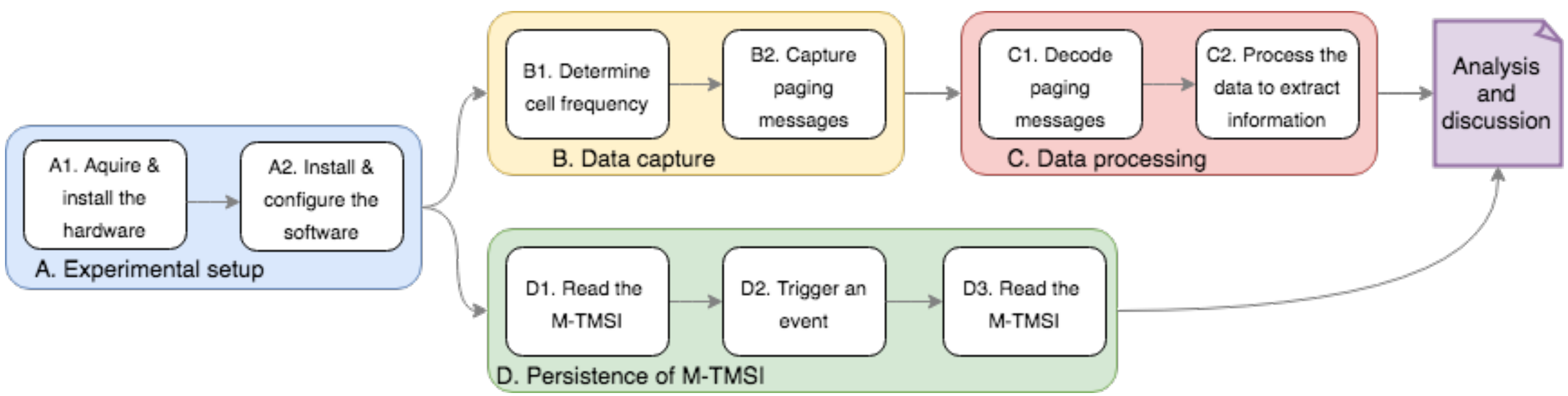
Roger Piqueras Jover
Bloomberg LP, New York, NY
rpiquerasjov@bloomberg.net

LTE Paging



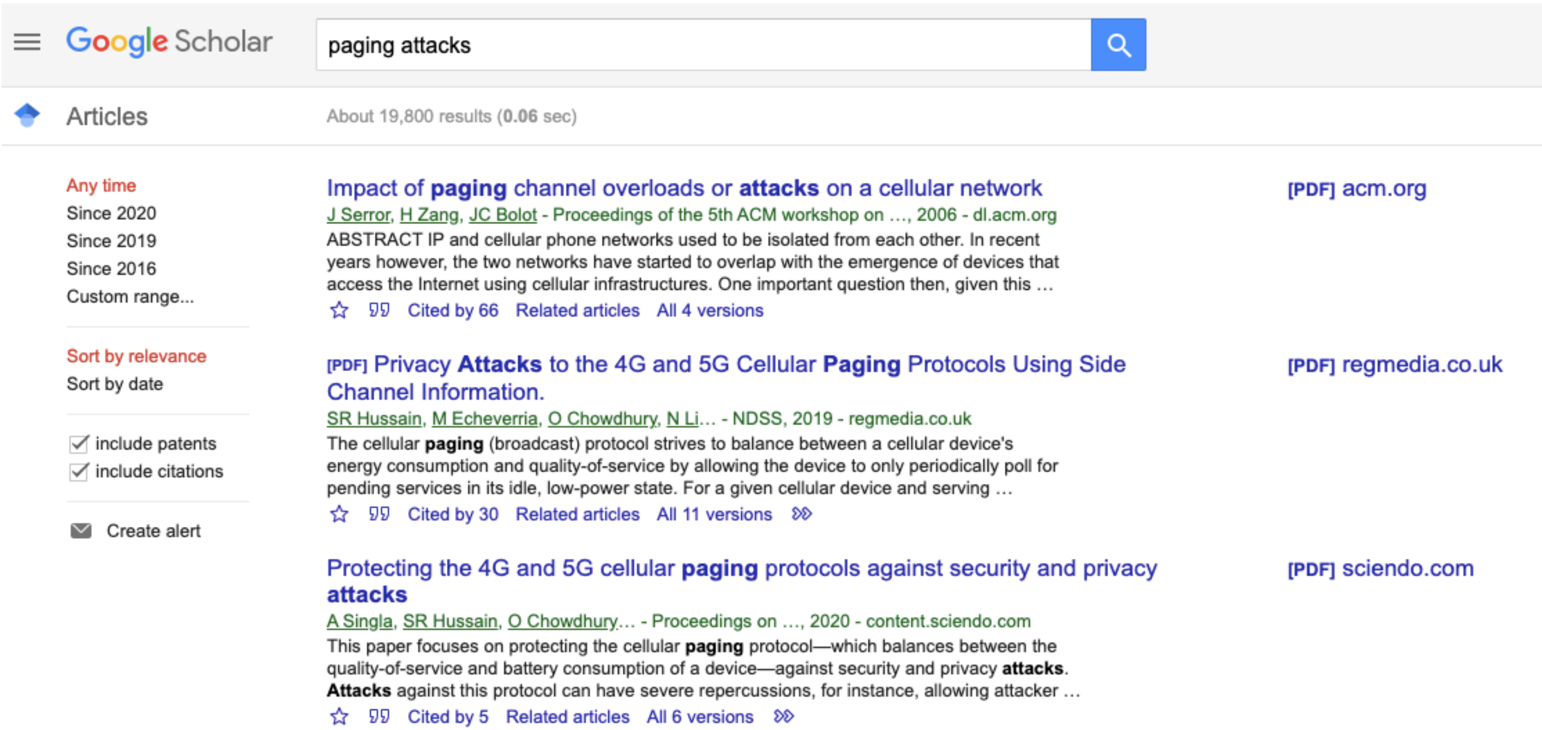

```
<PCCH-Message>
  <message>
    <c1>
      <paging>
        <pagingRecordList>
          <PagingRecord>
            <ue-Identity>
              <s-TMSI>
                <mmec>00111000</mmec>
                <m-TMSI>11010000001111110111001110010000</m-TMSI>
              </s-TMSI>
            </ue-Identity>
            <cn-Domain>
              <ps/>
            </cn-Domain>
          </PagingRecord>
        </pagingRecordList>
      </paging>
    </c1>
  </message>
</PCCH-Message>

7 bytes decoded.
*** DECODING SUCCESSFUL ***
```

Sørseth, C., Zhou, S.X., Mjølsnes, S.F. and Olimid, R.F., *Wireless Personal Communications*, 2019
Experimental analysis of subscribers' privacy exposure by LTE paging.

Many Publications and Results


Google Scholar

paging attacks

Articles

About 19,800 results (**0.06** sec)

Any time
Since 2020
Since 2019
Since 2016
Custom range...

Sort by relevance
Sort by date

include patents
include citations

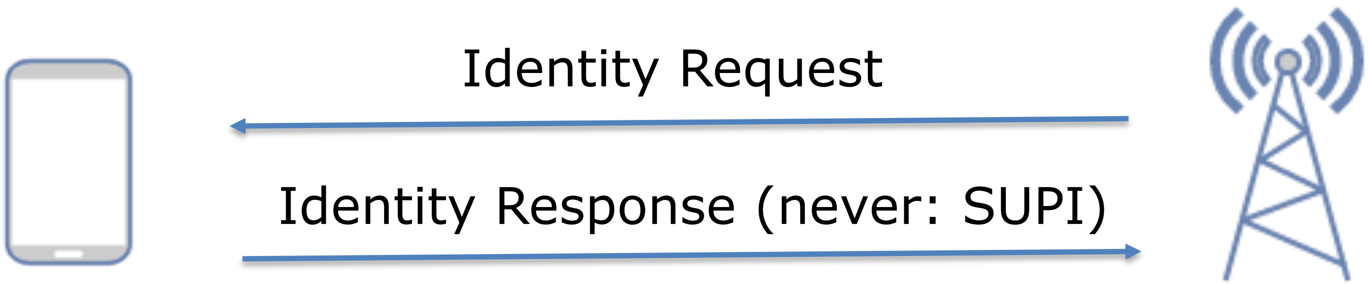
Create alert

Impact of **paging** channel overloads or **attacks** on a cellular network — [PDF] acm.org
J Serror, H Zang, JC Bolot - Proceedings of the 5th ACM workshop on …, 2006 - dl.acm.org
ABSTRACT IP and cellular phone networks used to be isolated from each other. In recent years however, the two networks have started to overlap with the emergence of devices that access the Internet using cellular infrastructures. One important question then, given this …
Cited by 66 Related articles All 4 versions

[PDF] Privacy **Attacks** to the 4G and 5G Cellular **Paging** Protocols Using Side Channel Information. — [PDF] regmedia.co.uk
SR Hussain, M Echeverria, O Chowdhury, N Li… - NDSS, 2019 - regmedia.co.uk
The cellular **paging** (broadcast) protocol strives to balance between a cellular device's energy consumption and quality-of-service by allowing the device to only periodically poll for pending services in its idle, low-power state. For a given cellular device and serving …
Cited by 30 Related articles All 11 versions

Protecting the 4G and 5G cellular **paging** protocols against security and privacy **attacks** — [PDF] sciendo.com
A Singla, SR Hussain, O Chowdhury… - Proceedings on …, 2020 - content.sciendo.com
This paper focuses on protecting the cellular **paging** protocol—which balances between the quality-of-service and battery consumption of a device—against security and privacy **attacks**. **Attacks** against this protocol can have severe repercussions, for instance, allowing attacker …
Cited by 5 Related articles All 6 versions

Changes in 5G

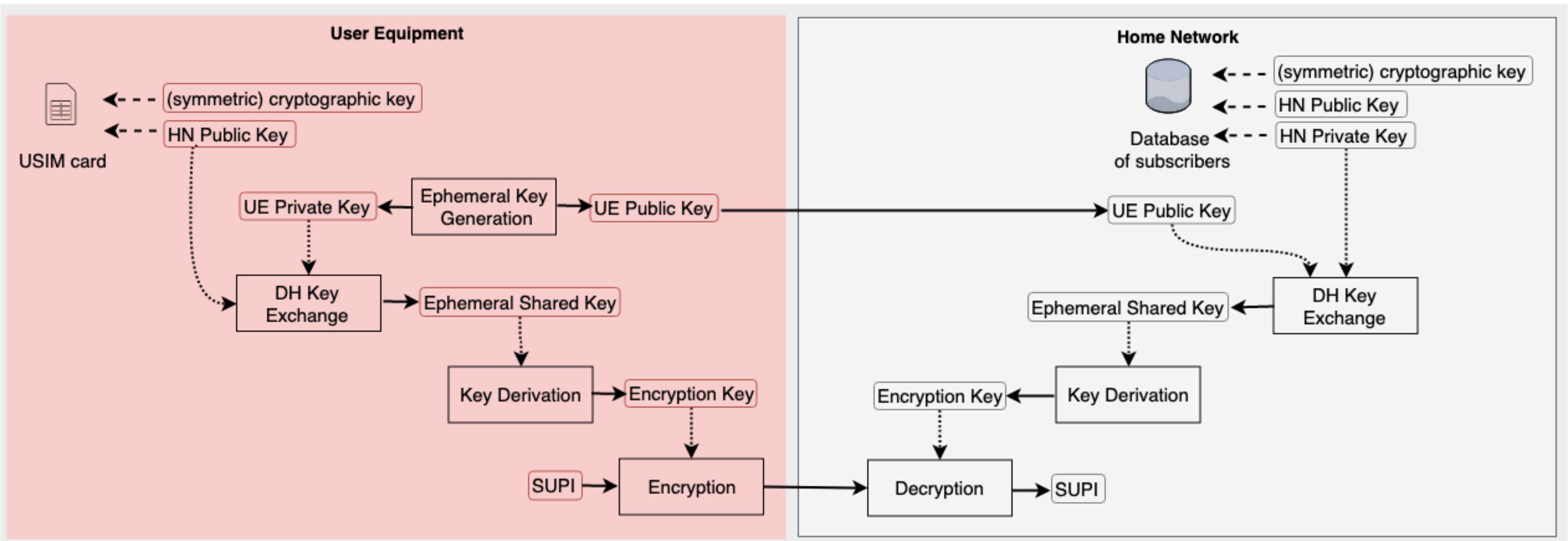


"In response to the Identifier Request message, the UE never sends the SUPI."

SUPI: Subscription Permanent Identifier

[3GPP TS 33.501 V16.4.0 (2020-09)]

5G – Concealment of SUPI (to SUCI)



Mjolsnes, S.F. and Olimid, R.F., IEEE CommMag 2019. *Private Identification of Subscribers in Mobile Networks: Status and Challenges*

SUPI: Subscription Permanent Identifier
SUCI: Subscription Concealed Identifier

5G – Concealment of SUPI (to SUCI)

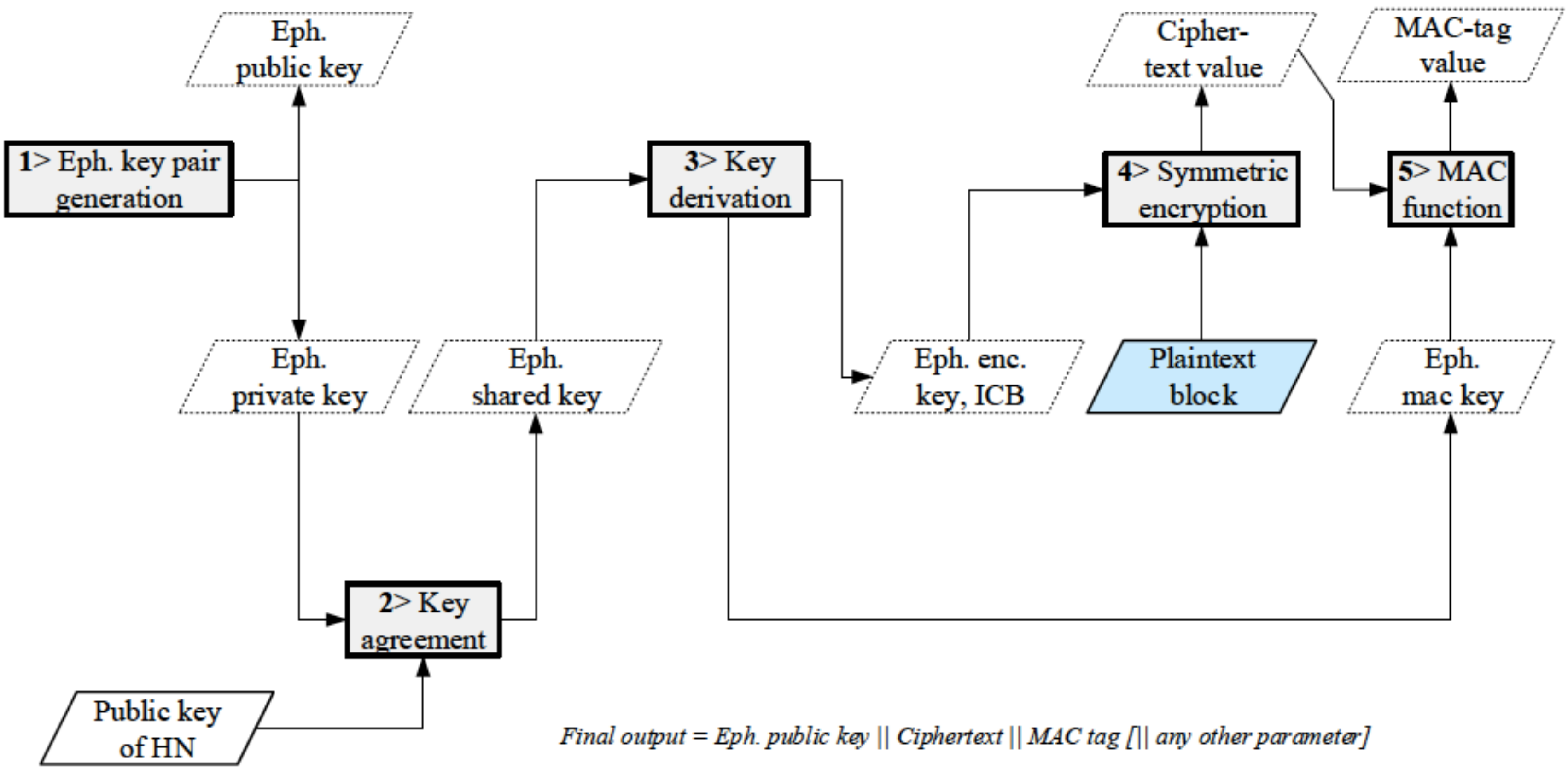


Figure C.3.2-1: Encryption based on ECIES at UE

ECIES: Elliptic Curve Integrated Encryption Scheme

[3GPP TS 33.501 V16.4.0 (2020-09)]

5G – Concealment of SUPI (to SUCI)

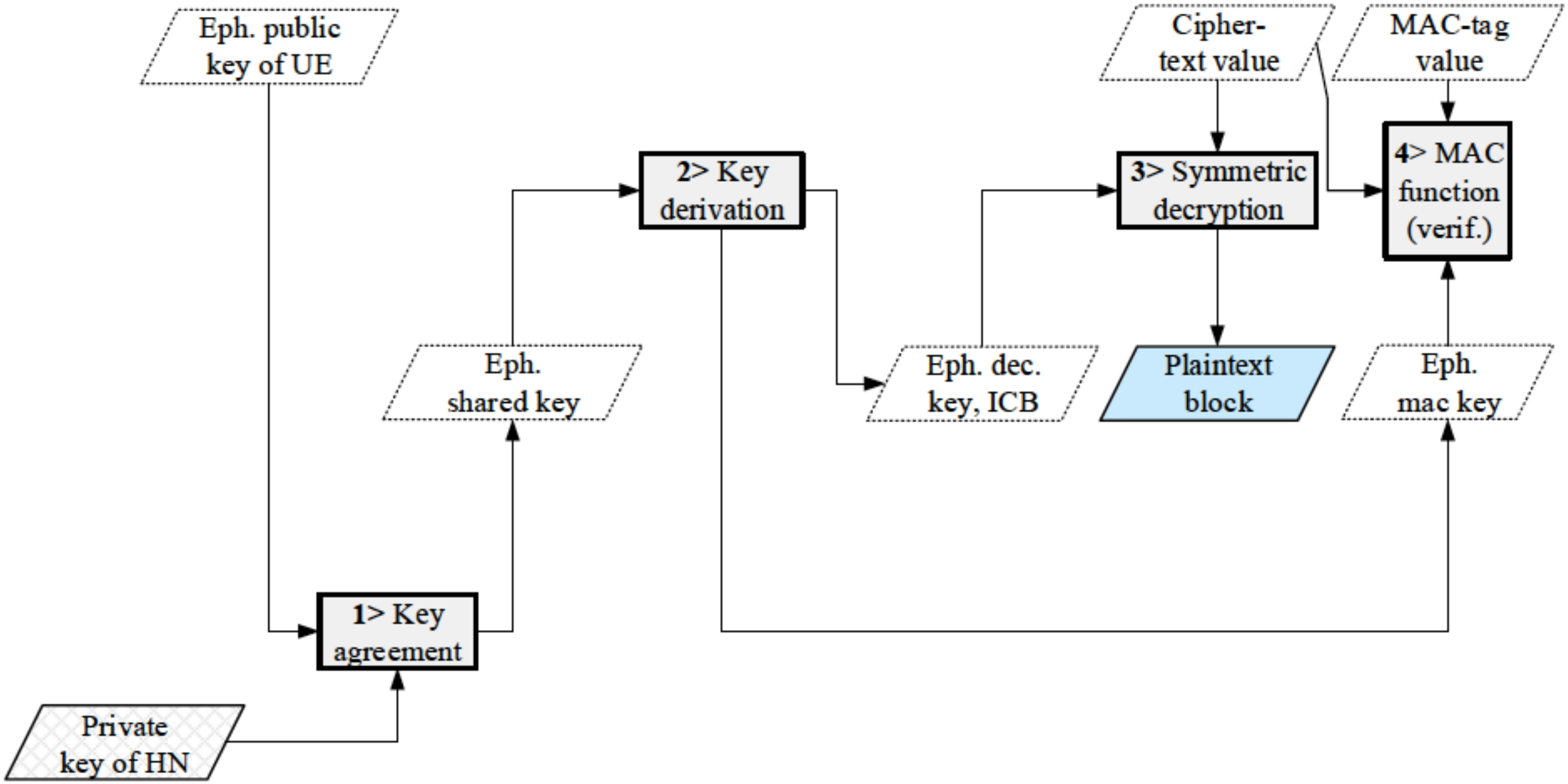


Figure C.3.3-1: Decryption based on ECIES at home network

ECIES: Elliptic Curve Integrated Encryption Scheme

[3GPP TS 33.501 V16.4.0 (2020-09)]

IMSI / SUPI Catching in 5G

- Downgrade to previous generations
- *Null-scheme*

“The UE shall generate a SUCI using "null-scheme" only in the following cases:
- if the UE is making an unauthenticated emergency session and it does not have a 5G-GUTI to the chosen PLMN,
or
- if the home network has configured "null-scheme" to be used, or
- if the home network has not provisioned the public key needed to generate a SUCI.”

[3GPP TS 33.501 V16.4.0 (2020-09)]

- Computational costs and difficult management caused by public key cryptography

IMSI / SUPI Catching in 5G

[Source: https://infosec.sintef.no/en/informasjonssikkerhet/2020/04/hacking-5g-network-infrastructure-imsi-catchers-and-hackathon/]

SINTEF INFOSEC
CYBERSECURITY RESEARCH GROUP

Home Blog About us Contact English

Hacking 5G Network Infrastructure – IMSI catchers and hackathon

POSTED ON: 14. April 2020
WRITTEN BY: Ravishankar Borgaonkar
COMMENTS: 1
CATEGORISED IN: Ukategorisert
TAGGED AS: 5g

Fake Base Station problem in 5G

Continuing with the previous blogpost, we discuss the problem o

WIRED BACKCHANNEL BUSINESS CULTURE GEAR MORE SIGN IN SUBSCRIBE

Get Unlimited WIRED Access SUBSCRIBE

LILY HAY NEWMAN SECURITY 08.03.2019 07:00 AM

5G Is Here—and Still Vulnerable to Stingray Surveillance

5G was supposed to offer new protections against so-called stingray surveillance devices. New research shows it's anything but.

[Source: https://www.wired.com/story/5g-security-stingray-surveillance/]

IMSI / SUPI Catching in 5G

5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol

Syed Rafiul Hussain
Purdue University
hussain1@purdue.edu

Mitziu Echeverria
University of Iowa
mitziu-echeverria@uiowa.edu

Imtiaz Karim
Purdue University
karim7@purdue.edu

Omar Chowdhury
University of Iowa
omar-chowdhury@uiowa.edu

Elisa Bertino
Purdue University
bertino@purdue.edu

ABSTRACT

The paper proposes 5GReasoner, a framework for property-guided formal verification of control-plane protocols spanning across multiple layers of the 5G protocol stack. The underlying analysis carried out by 5GReasoner can be viewed as an instance of the model checking problem with respect to an adversarial environment. Due to an effective use of behavior-specific abstraction in our manually extracted 5G protocol, 5GReasoner's analysis generalizes prior analyses of cellular protocols by reasoning about properties not only regarding packet payload but also multi-layer protocol interactions. We instantiated 5GReasoner with two model checkers and a cryptographic protocol verifier, lazily combining them through the use of abstraction-refinement principle. Our analysis of the extracted 5G protocol model covering 6 key control-layer protocols spanning across two layers of the 5G protocol stack with 5GReasoner has identified 11 design weaknesses resulting in attacks having both security and privacy implications. Our analysis also discovered 5 previous design weaknesses that 5G inherits from 4G, and can be exploited to violate its security and privacy guarantees.

1 INTRODUCTION

The imminent deployment of the fifth generation (5G) cellular network has created a lot of enthusiasm in both industry and academia particularly due to its promise of enabling new applications such as smart vehicles and remote robotic surgery. 5G is not only envisioned as a replacement of home broadband Internet but also is expected to have impact in the military battlefield and emergency management by improving situational awareness. All these potential novel and critical applications of 5G can be attributed to its following enhancements over 4G LTE: (1) Improvements in the physical-layer technologies enabling the support of large numbers of devices with substantially improved bandwidth; (2) Robust security posture due to the introduction of security measures in the upper-layer of the 5G protocol stack. The 5G standard, however, has opened the door to a wide array of new security challenges stemming from: (i) New security policies that are not formally verified against adversarial assumptions; (ii) Retaining security mechanisms from 4G Long Term Evolution (LTE) and its predecessors. *This paper thus aims to develop highly automated approaches enabling property-guided formal verification of control-plane protocols of the 5G protocol stack*

Thank you!