CENTER FOR CYBER SECURITY

CSP-lab
Cyber Security and Privacy Lab

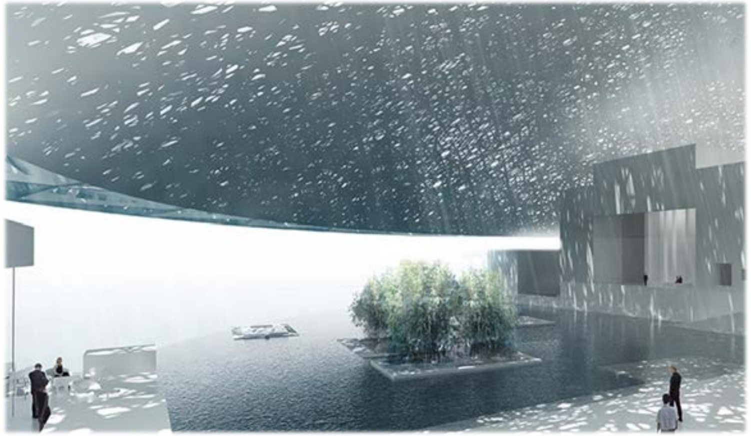
جامعة نيويورك أبوظبي
NYU ABU DHABI

What could possibly go wrong? Security and Privacy in 5G/nextG Mobile Networks

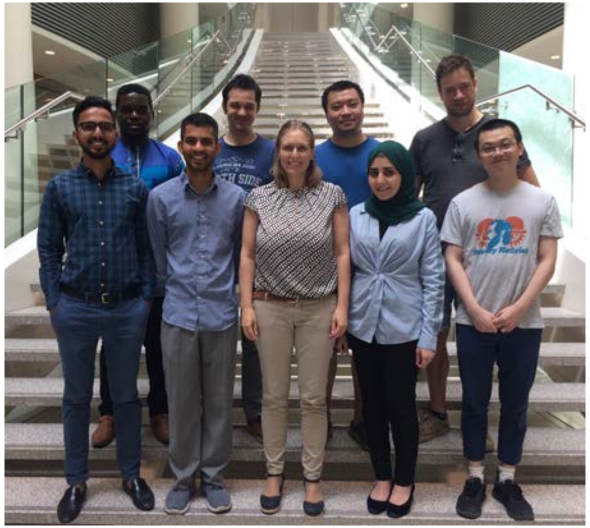
Christina Pöpper, New York University Abu Dhabi

June 6, 2023

About






About

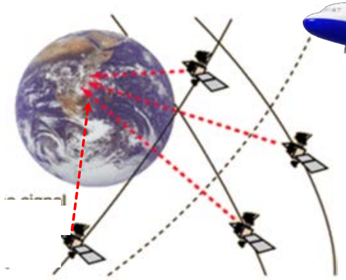
جامعة نيويورك أبوظبي
NYU | ABU DHABI

CSP-lab
Cyber Security and Privacy Lab

CENTER FOR
CYBER SECURITY

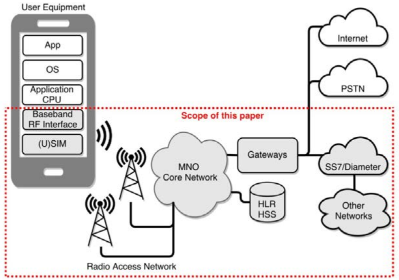
- Computer Science Faculty at NYUAD, Ph.D. from ETH Zurich
  - Leading the Cyber Security & Privacy (CSP) Lab since 2016
  - Director of Research at Center of Cybersecurity at NYUAD since 2019
- 15 years of research experience in **cyber security** and **wireless security**
  - 8 years of in **mobile/cellular security**

Secure Localization & Aviation



NextGEN ADS-B

Mobile/Cellular Network Security



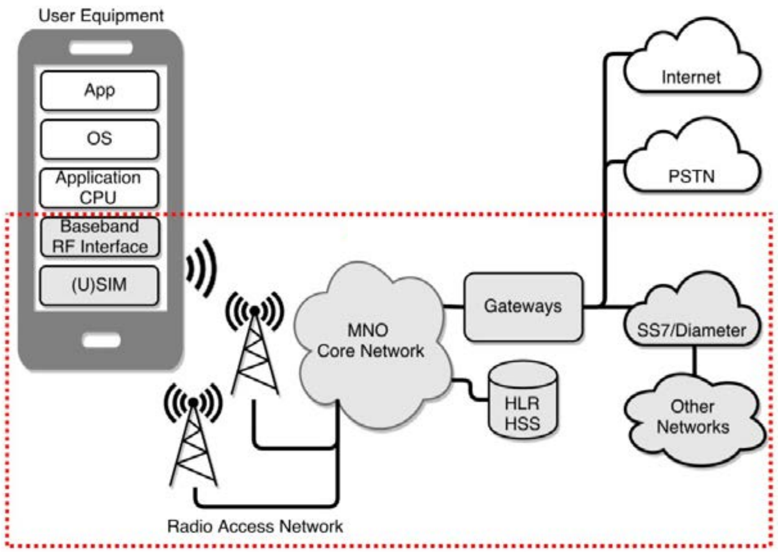
lte

5G

Anonymity & Privacy

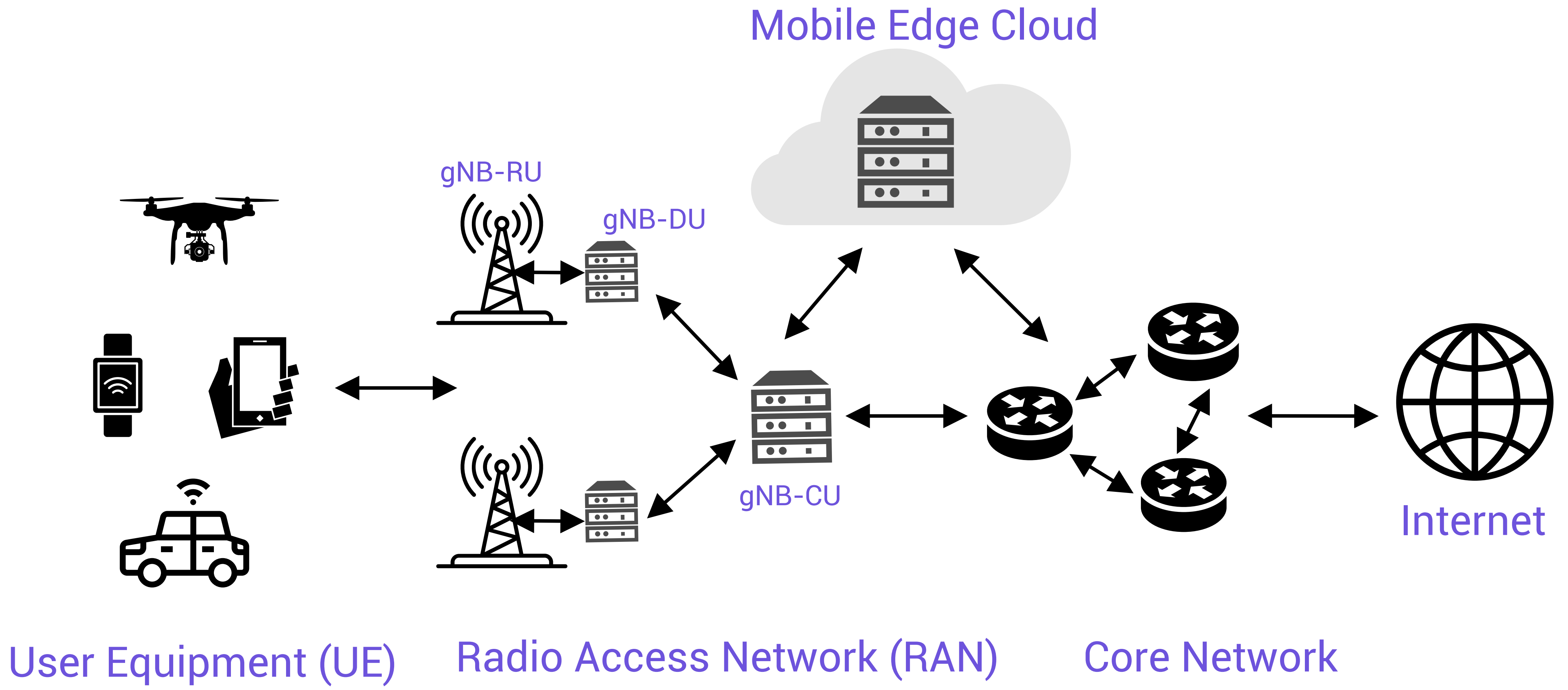
Tor

Mobile/Cellular Network Security

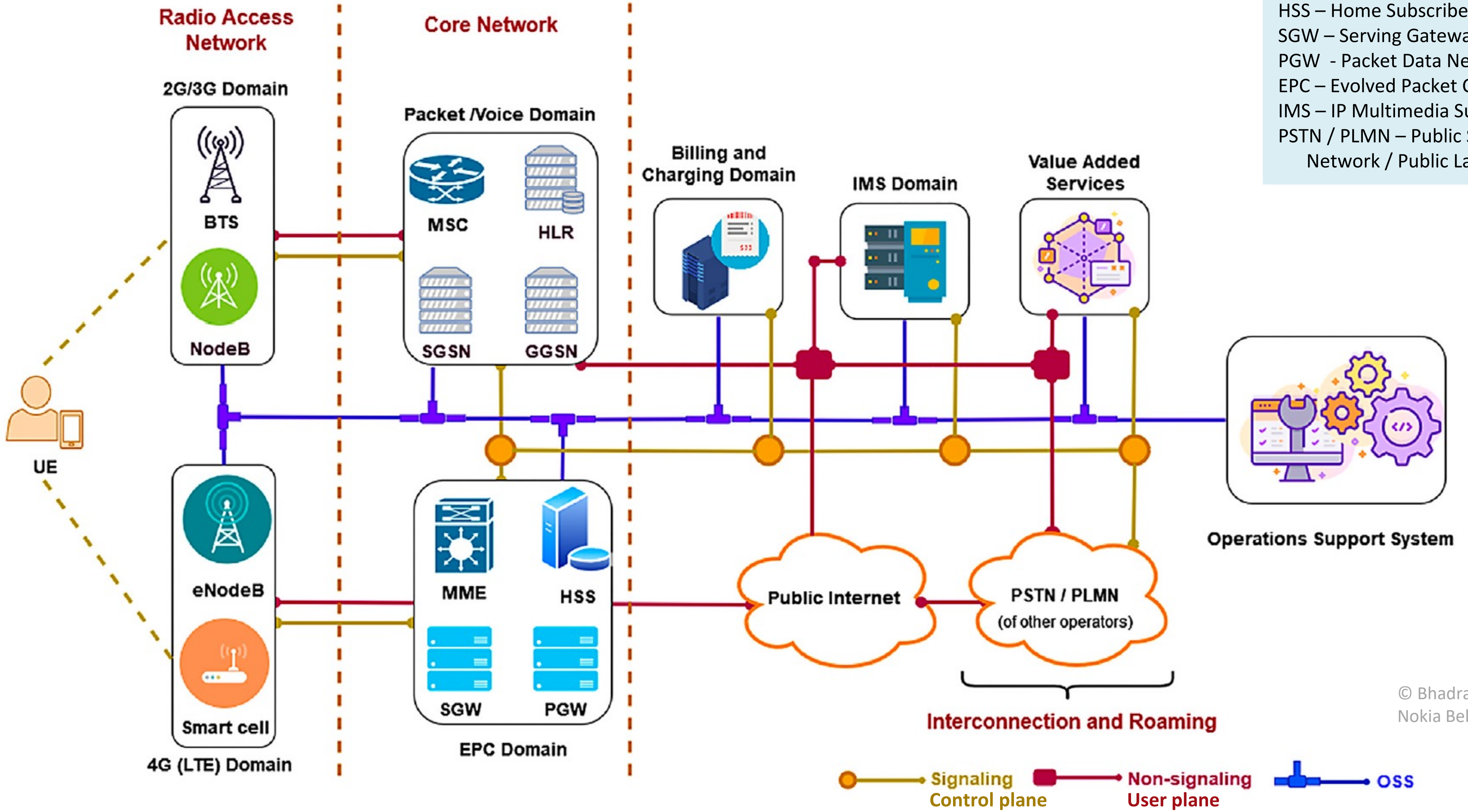


Mobile Network Security

Cellular / Telecommunications Networks



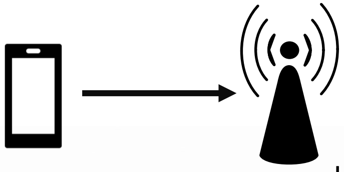
Cellular Network Topology



MSC – Mobile Switching Center
HLR – Home Location Register
SGSN – Serving GPRS Support Mode
GGSN – Gateway GPRS Support Mode
MME – Mobility Management Entity
HSS – Home Subscriber Server
SGW – Serving Gateway
PGW - Packet Data Network Gateway
EPC – Evolved Packet Core
IMS – IP Multimedia Subsystem
PSTN / PLMN – Public Switched Telephone Network / Public Land Mobile Network

Security in Cellular Networks – A Quick Pass through the Generations

- Security issues & vulnerabilities



1G (1980): Audio only w/o security or privacy guarantees — Voice Call/Analog

2G (1990): One-way authentication, weak A5/1 | GEA-1 — SMS/Digital

3G (2000): IP traffic vulnerabilities (virus, malware), encryption key issues — Web Applications/Wideband

4G (2010): MAC-layer vulnerabilities, missing integrity protection, threats from new services/ devices, user tracking — Mobile Applications/Gbps

5G (2020): Vulnerabilities in NFV, SDN, and cloud techniques, openness of the network — IoT, VR/AR, Smart City

6G (2030): ? Security issues in AI-powered technology, intelligent radios, quantum attacks — Autonomous systems, Multi-sensory XR, Wireless brain computer interaction

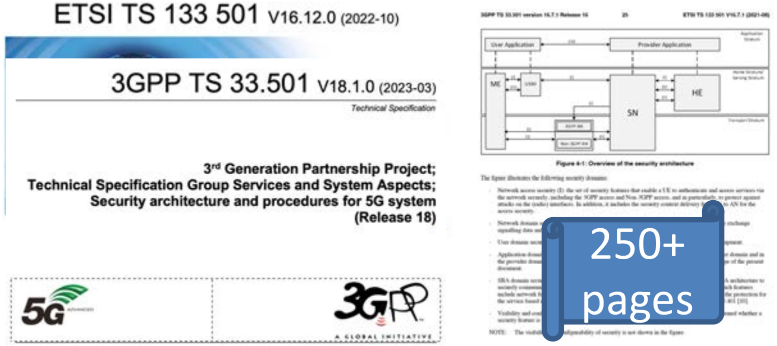
Cellular Network Entities and Development Phases

Specification → Implementation → Deployment

Specification & Standarization Bodies

Vendors

Network Operators


ETSI TS 133 501 V16.12.0 (2022-10)

3GPP TS 33.501 V18.1.0 (2023-03)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security architecture and procedures for 5G system
(Release 18)

250+ pages

Our Research Contributions

Specification → Implementation → Deployment

aLTEr-Attacks: Breaking LTE on Layer Two IEEE S&P'19

IMP4GT: IMPersonation Attacks in 4G NeTworks NDSS'20

Call Me Maybe: Eaves-dropping Encrypted LTE Calls With ReVoLTE USENIX Sec'20

LTE Security Disabled – Misconfiguration in Commercial Networks ACM WiSec'19

4G/LTE

5G/NR

Don't hand it Over: Vulnerabili-ties in 5G Handover Procedures ACSAC'21

5G SA Security Testing Frame-work for 5G UEs. WiSec'23

5G SUCI-Catchers: Still catching them all? ACM WiSec'21

Abusing 5G's Warning and Emergency Systems ACSAC'22

Extracting User Locations by SMS Timings. Usenix Sec'23

Logos: © Katharina Kohls

Security Requirements (5G)

WiSec'23

Bidding Down Attacks and Mitigations on 5G and 4G

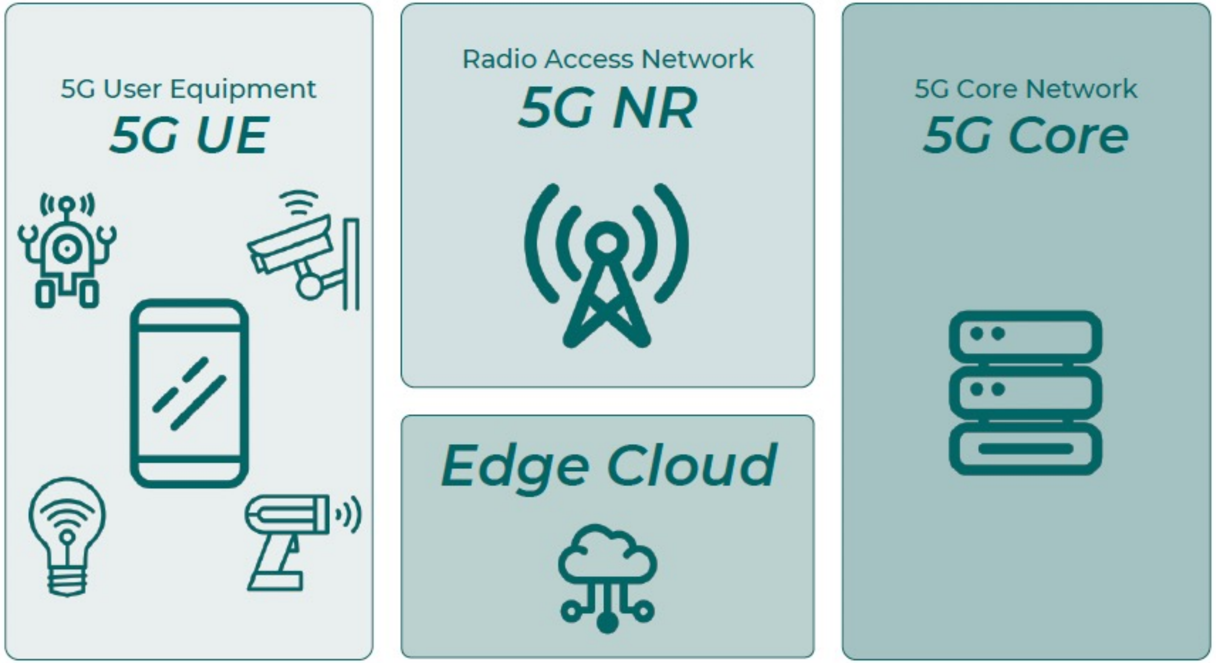
Mitigation of downgrading attacks

Mutual Authentications

Traffic Confidentiality

Signaling Integrity

Identity & Location Privacy



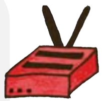
Source: wenovator

Secure storage & processing of subscription credentials

Security Enhancements from 4G to 5G

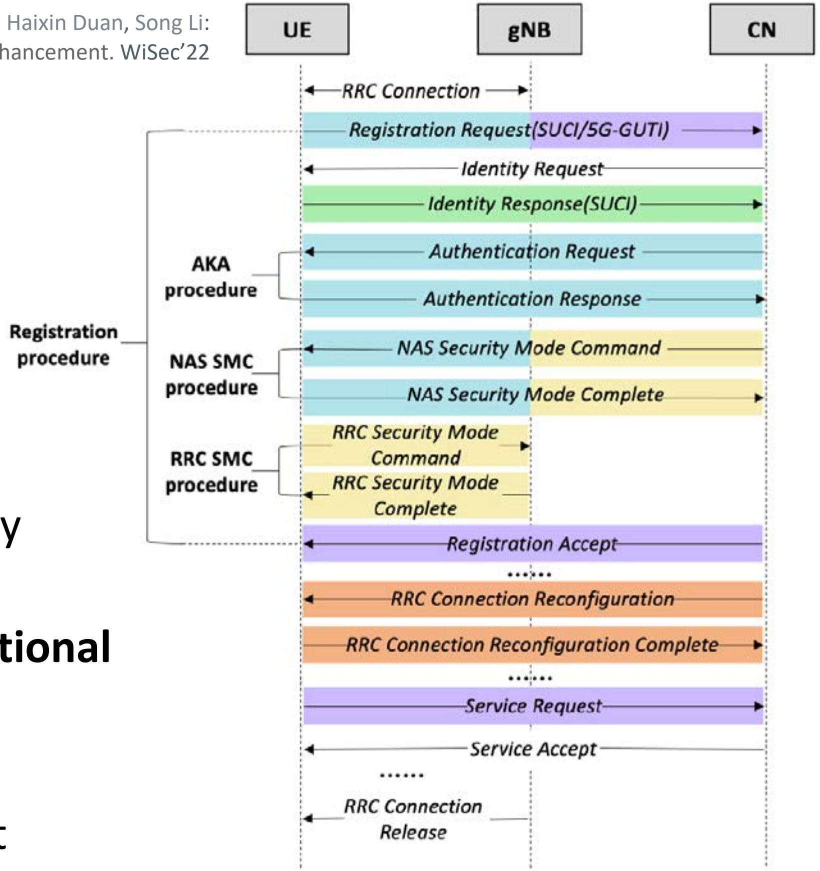
Issue	4G	5G Enhancement	Mitigated Threat
Confidentiality & Integrity Protect.	*Control Layer*: Encryption & Integrity Protection *User Plane*: Encryption	+ Mandatory support for User Plane Integrity Protection	If used: Prevention of tampering with user data (aLTEr/IMP4GT-like attacks)
Subscriber Privacy	SUPI sent in plaintext No guidelines for updating temp. identities (GUTI)	SUPI → SUCI concealment Well defined timing of 5G-GUTI redistribution	Large-scale IMSI-catchers, location exposure, user tracking
NAS Security	Initial NAS messages are sent in plaintext	Confidentiality protection of initial NAS messages	Network spoofing, message hijacking, DoS attacks





https://www.gsma.com/security/securing-the-5g-era/

© Shiyue Nie, Yiming Zhang, Tao Wan, Haixin Duan, Song Li: Measuring the Deployment of 5G Security Enhancement. WiSec'22



5G Security Features

5G security features:

Protection of initial NAS messages
5G-GUTI reallocation
SUPI concealling
User plane security activation
Security algorithm

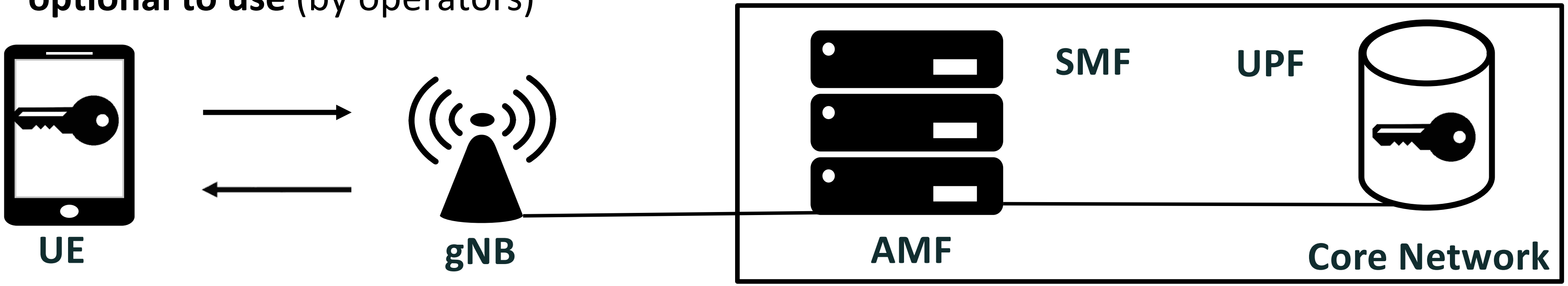
3GPP TS 33.501 (v16)

Control Plane Protection:

- Mandatory Integrity Protection (supported by products and used by operators)
- Confidentiality is mandatory to be supported (by products), but **optional to use** (by operators)

User Plane Protection:

- Mandatory support for Confidentiality and Integrity Protection, but **optional to use** (by operators)

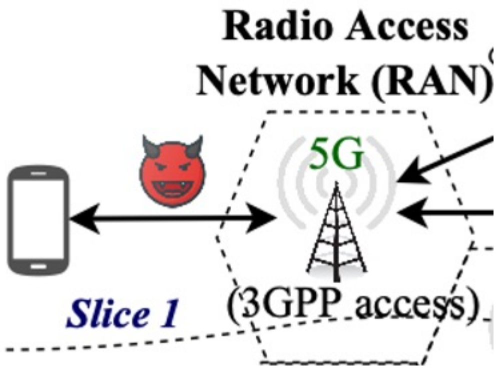


General Challenges for 5G/6G Security

- Significant advances made in recent years in cellular security.
  - elaborate security mechanisms standardized for 5G

- But: Cellular security remains a challenge. Reasons (learned from the past):
  - network generation overlap and backwards compatibility requirements
  - involvement of many parties (government, operators, device manufacturers, users)
  - (many) broadcast messages (currently) not integrity protected
  - complex and huge standards
  - substantial internetworking and peripherals (WiFi, IoT, UAVs, …)
  - constant necessity of updated tools and software
  - more complex interactions lead to more widespread attacks
  - …

Yongdae Kim @ AsiaCCS'22



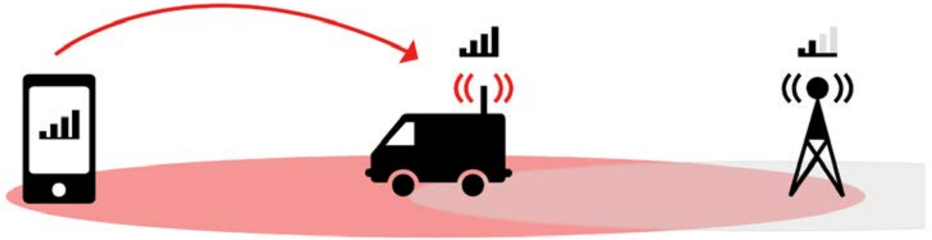
© Syed Rafiul Hussein

Mobile Network Threat Landscape

Attacks on Cellular Networks

Radio-layer Attacks on Cellular Networks

- Jamming | DoS | Downgrading
- IMSI catchers | Stingrays | False Base Stations | Cell Site Simulators



Source: https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks

Higher-layer Attacks on Cellular Networks

- Phishing, Smishing, Spamming
- RoboCalls, Silent SMS
- Malware (Simjacker, WibAttack), Viruses (Flubot)
- Potential of AI/ML attacks

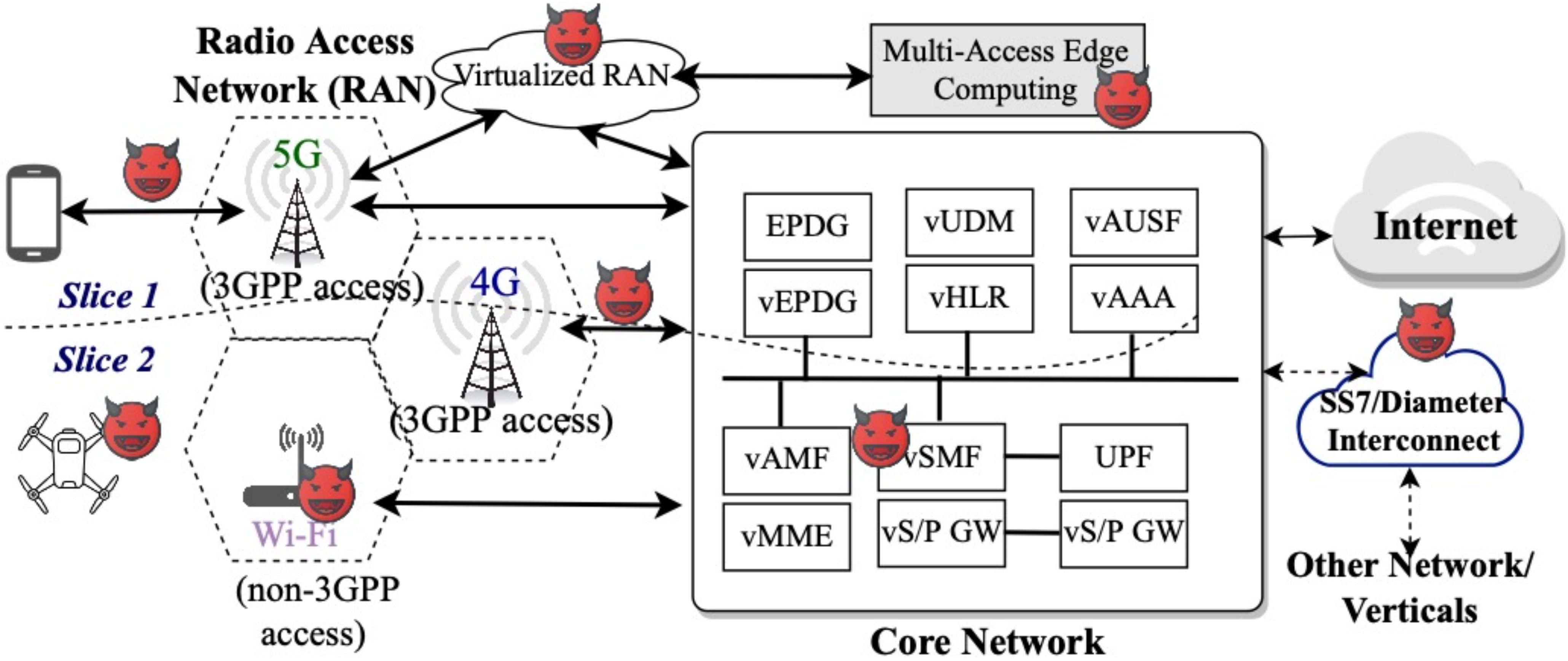
Categories of attacks:

- Denial of service & Service downgrading
- Presence testing & Location tracking
- Communication interception (2G/3G)

Categories of attacks:

- Targeting mobile users
- Targeting mobile apps
- Targeting mobile devices
- Targeting network/core/ operator

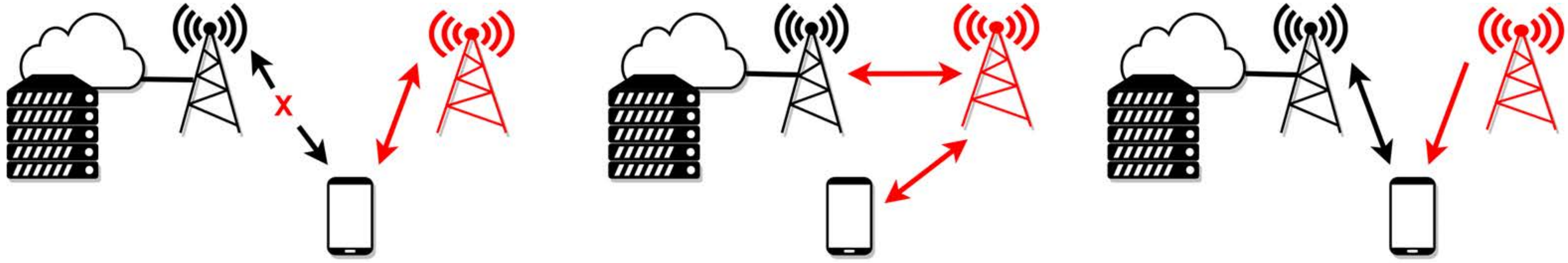
Threat Landscape on Cellular Networks



Threat Modeling for Mobile / Cellular Communications

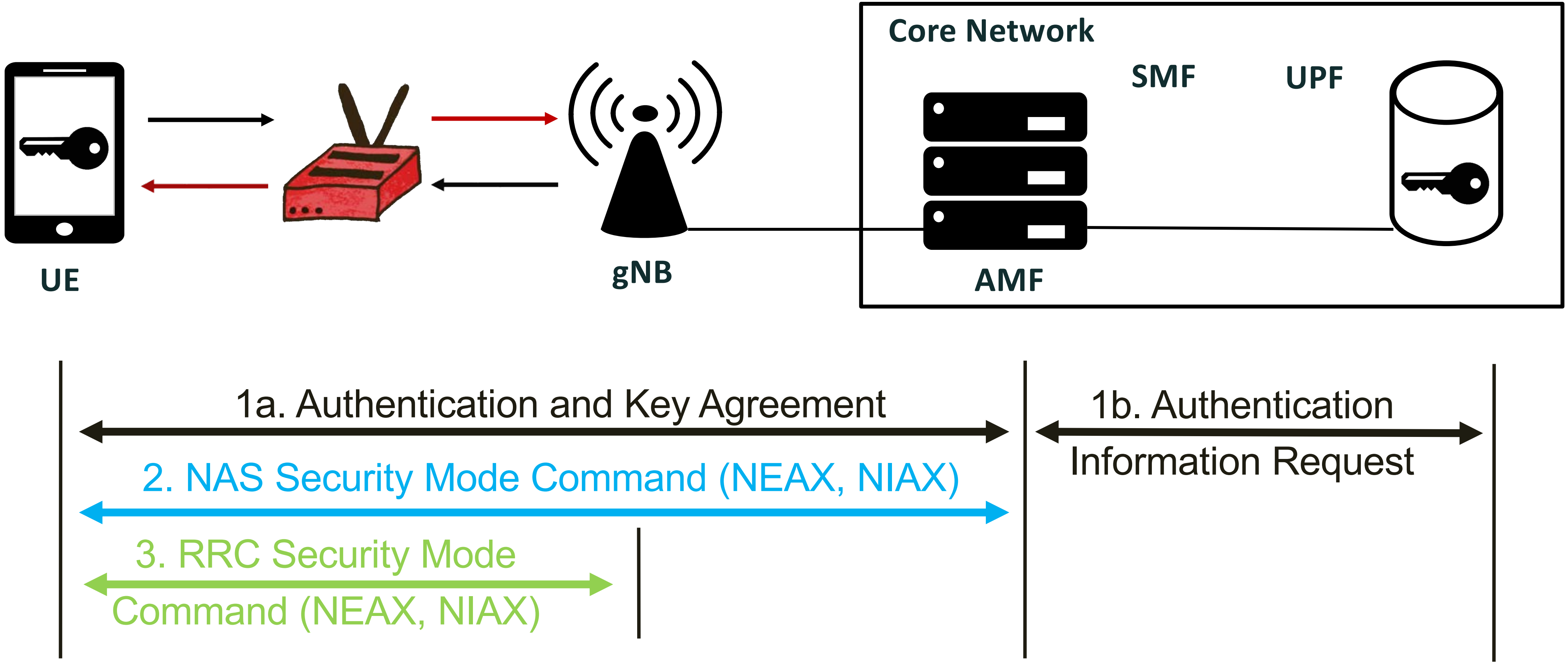
Attack Mounting			Attack Progression				Attack Results	
Reconnaissance	**Initial Access**	**Persistence**	**Discovery**	**Lateral Access**	**Standard Protocol Misuse**	**Defense Evasion**	**Collection**	**Impact**
Perimeter mapping of network infrastructure	Access from UE	Infecting UE software or hardware	Operator network mapping	Exploiting interfaces within the operator network	SS7-based techniques	Stealth scanning	Administrator credentials	Location tracking
Perimeter mapping for mobiles	SIM-based compromise	Infecting network elements	Core network function scanning	Exploiting roaming and interconnection	Diameter-based techniques	Firewall bypass	Operator-specific identifiers	Personal information disclosure
Out-of-band intelligence gathering	Access from radio access network	Command and control channels	Internal intelligence gathering	Exploiting interworking	Routing information querying techniques	Denylist evasion	Operator data	Mass information gathering
	Access from inside the operator network	Exploiting hard-to-repair vulnerabilities	Internal UE scanning	Core-network access from radio network	GTP-based techniques	Malware anti-detection techniques	User credentials	Unwanted communication
	Access from partner mobile network	Knowledge of keys and credentials		Exploiting platform- and service-specific vulnerabilities	IP-based techniques	Signaling-protocol downgrading	User-specific identifiers	Call, message and data interception
	Access from operator's IP network infrastructure			Exploiting implementation flaws in 3GPP protocols	SIP-based techniques	Radio-link downgrading and redirection	Communication metadata	Failure of mobile network as trsuted channel
	Access from the public Internet				AKA-related techniques			Billing discrepancies
	Compromised insiders and human errors				Cryptographic techniques			Denial of Service
	Supply chain attacks							

Adversary Categories

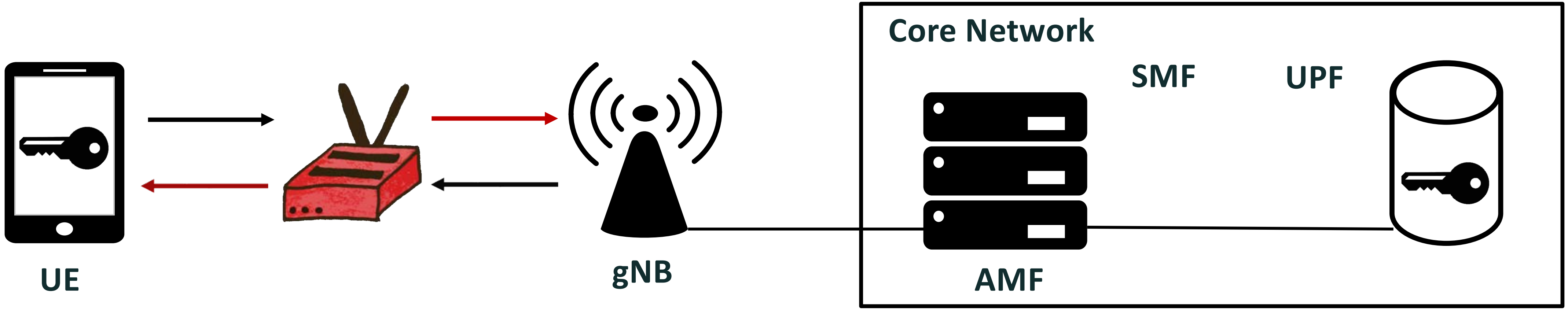


(a) False Base Station (b) Man-in-the-Middle (c) Signal Overshadowing

Types of MITM/Relay Cellular Attackers



Types of MITM/Relay Cellular Attackers



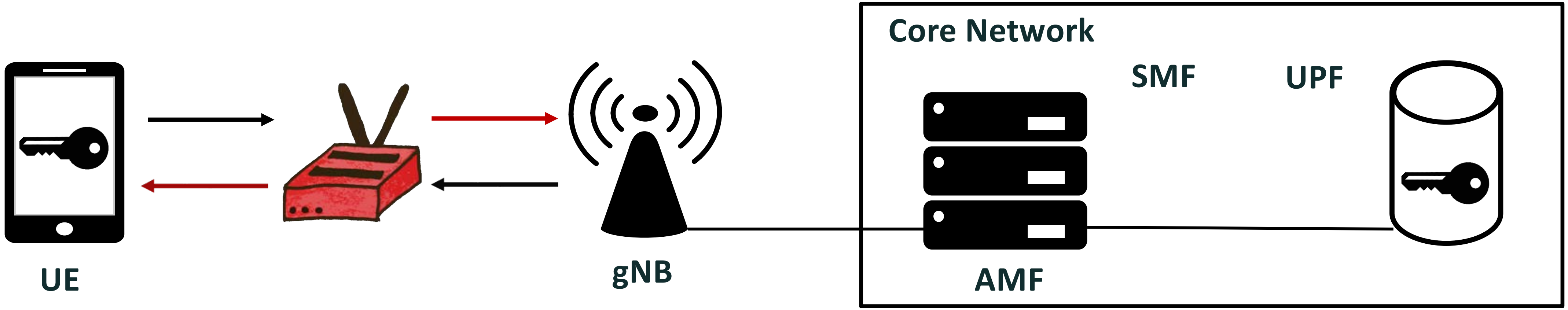
1) Repeater/Forwarder
   (on the PHY-layer)
   → boosting signal strength

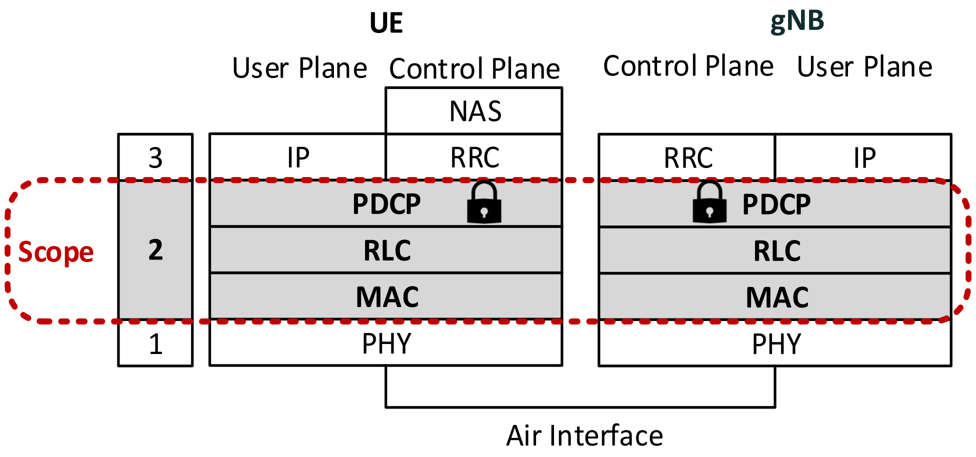
- Leaking plaintext identities, payload (2G-3G)
- Fingerprinting of user activities (browsing, videos)

Types of MITM/Relay Cellular Attackers

Rupprecht, Kohls, Holz, Pöpper: **Breaking LTE on Layer Two** IEEE S&P, 2019 (**aLTEr**)

Rupprecht, Kohls, Holz, Pöpper: **IMP4GT: IMPersonation Attacks in 4G NeTworks,** NDSS, 2020

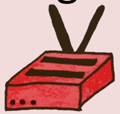




1) Repeater/Forwarder (on the PHY-layer) → boosting signal strength

2) Relay (on the MAC-layer) → signals to bits, (de)modulation, connections, forwarding on PDCP/RRC layers

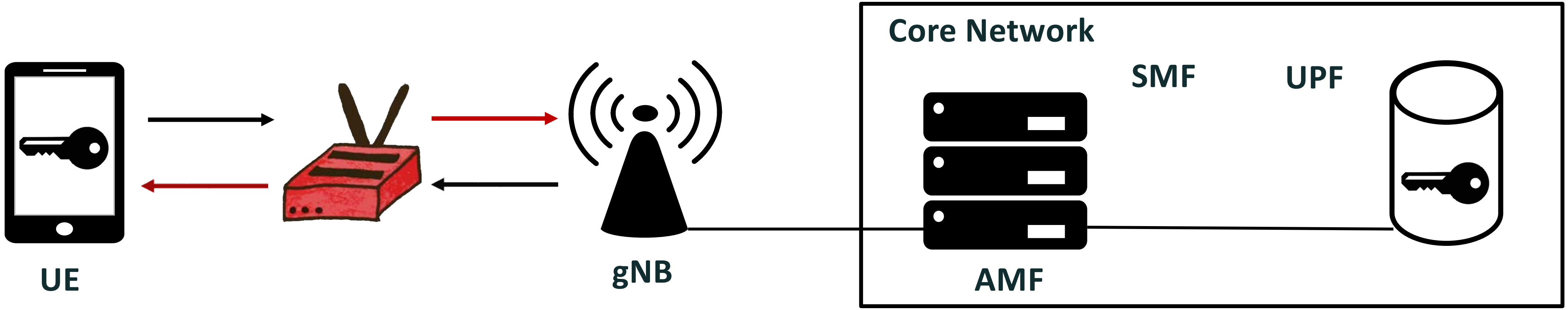
- Tampering with packets, recover data
- Impersonate users (in 4G or if user-plane traffic is not integrity-protected)



Types of MITM/Relay Cellular Attackers

Rupprecht, Kohls, Holz, Pöpper: **Breaking LTE on Layer Two** IEEE S&P, 2019 (aLTEr)

Rupprecht, Kohls, Holz, Pöpper: **IMP4GT: IMPersonation Attacks in 4G NeTworks**, NDSS, 2020



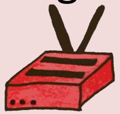
AdaptOver (LTE & 5G-NSA, MobiCom2022):

- decode, overshadow & inject arbitrary messages over the air in up- and downlink direction between network and UE

1) Repeater/Forwarder (on the PHY-layer)
   → boosting signal strength

2) Relay (on the MAC-layer)
   → signals to bits, (de)modulation, connections, forwarding on PDCP/RRC layers

- Tampering with packets, recover data
- Impersonate users (in 4G or if user-plane traffic is not integrity-protected)



@merlinchlosta

WiSec'21

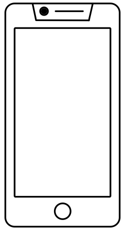
5G SUCI Catchers: Still Catching them all?

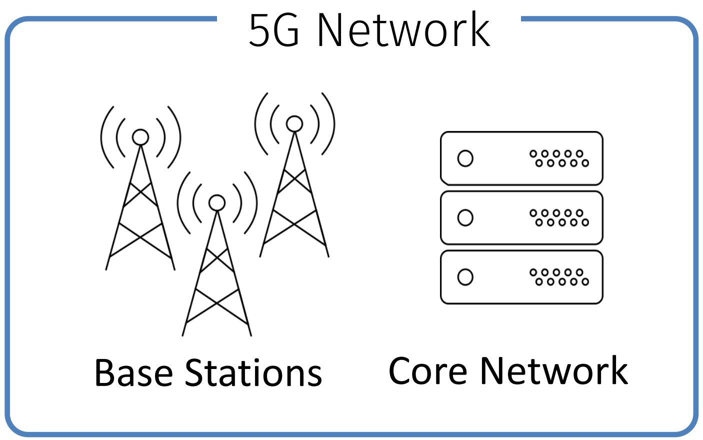
Mobile Network Privacy

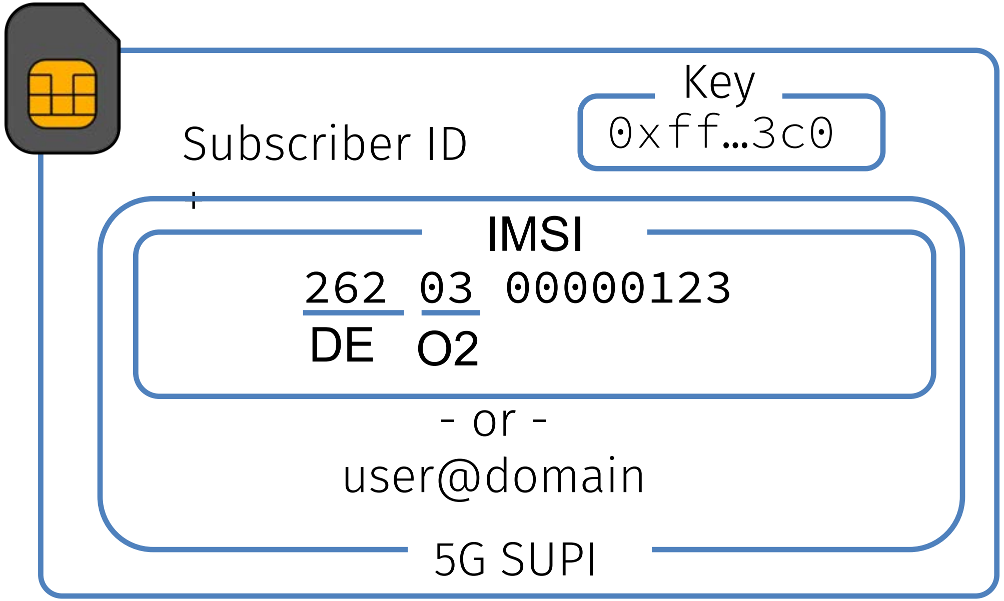
5G SUCI Catching

https://www.youtube.com/watch?v=PhLpC1cN_Rg

Identification in 5G Mobile Networks

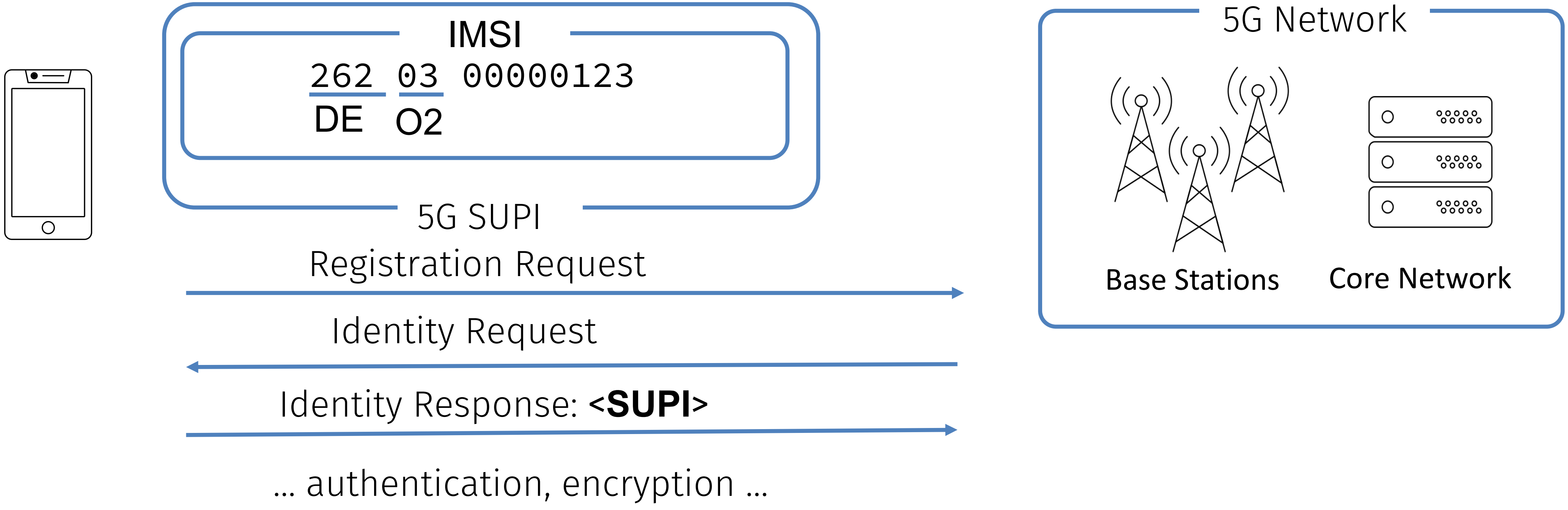






Chlosta, Rupprecht, Pöpper, Holz: **5G SUCI Catchers: Still catching them all?** ACM WiSec, 2021

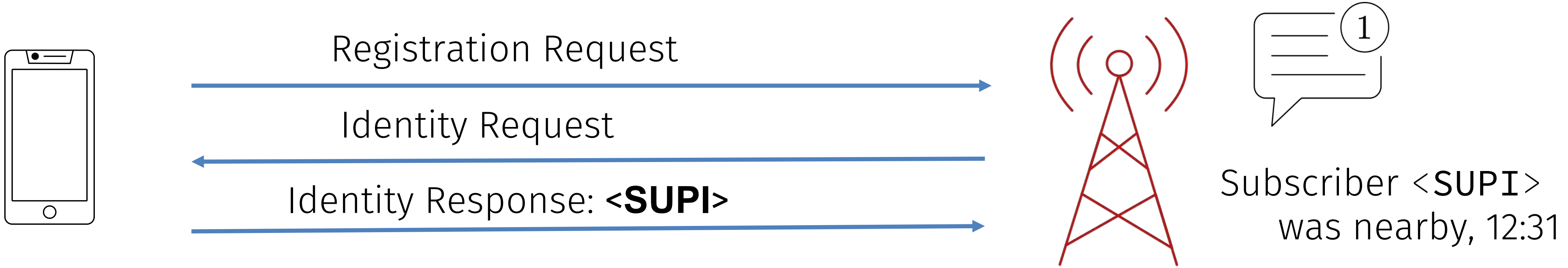
Identification in 5G Mobile Networks



… authentication, encryption …

Chlosta, Rupprecht, Pöpper, Holz: **5G SUCI Catchers: Still catching them all?** ACM WiSec, 2021

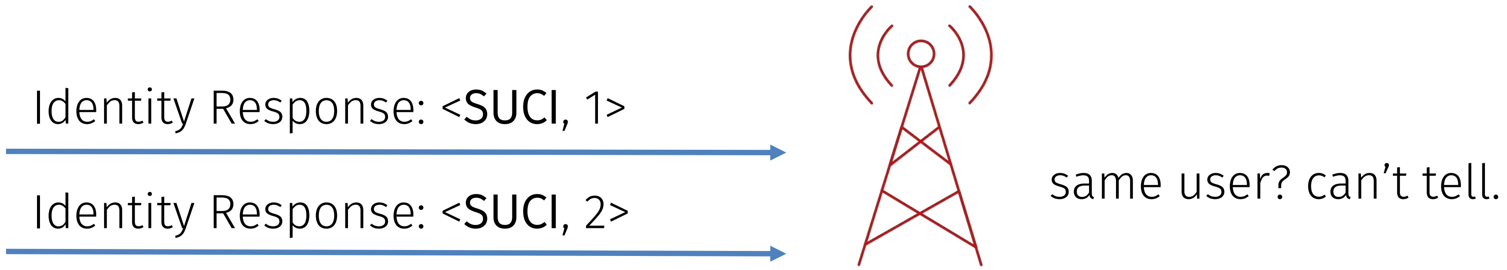
4G IMSI/SUPI Catchers [Fake Base Stations]



5G SUPI Concealment: SUCI 🍣

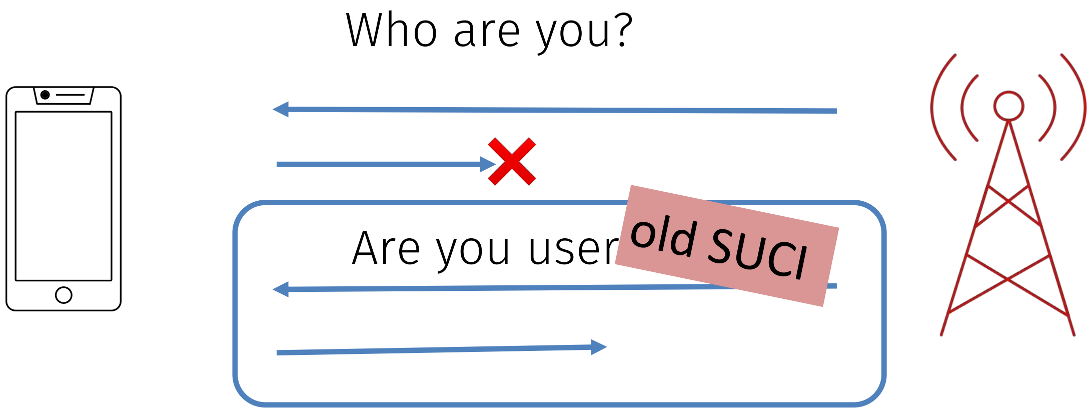
*"3GPP decided that SUCI is pronounced as **SU-SHI**"*
Nori: Concealing the Concealed Identifier in 5G
John Preuß Mattsson and Prajwol Kumar Nakarmi, ARES 2021

Operator Public Key + Ephemeral Key + SUPI / IMSI



Chlosta, Rupprecht, Pöpper, Holz: **5G SUCI Catchers: Still catching them all?** ACM WiSec, 2021

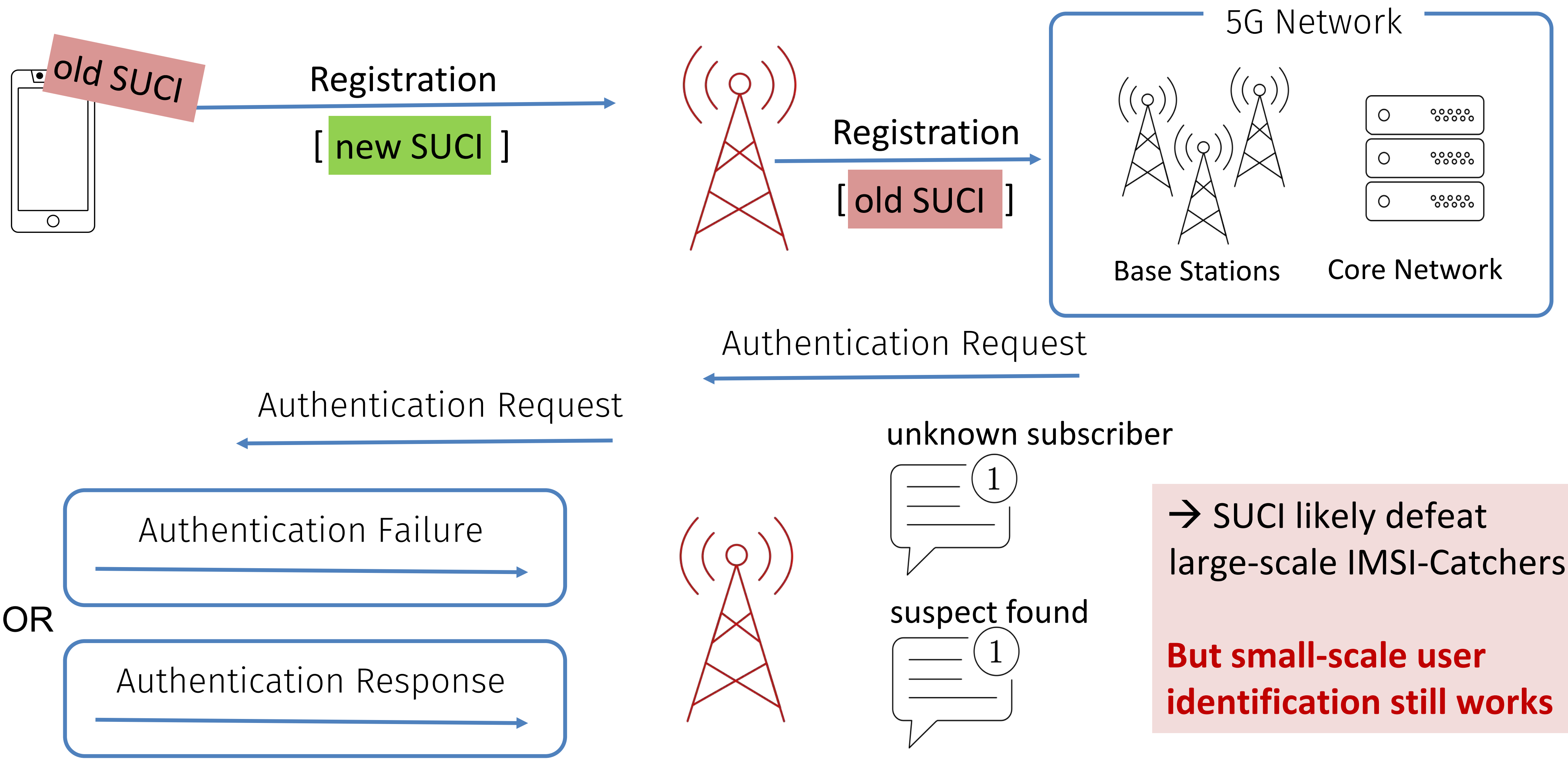
SUCI-Catching



- detective work 🚐📡🕵🏼

Chlosta, Rupprecht, Pöpper, Holz: **5G SUCI Catchers: Still catching them all?** ACM WiSec, 2021

Linking SUCIs



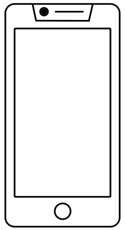
→ SUCI likely defeat large-scale IMSI-Catchers

But small-scale user identification still works

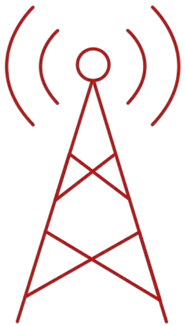
Experimental Evaluation

WiSec'21

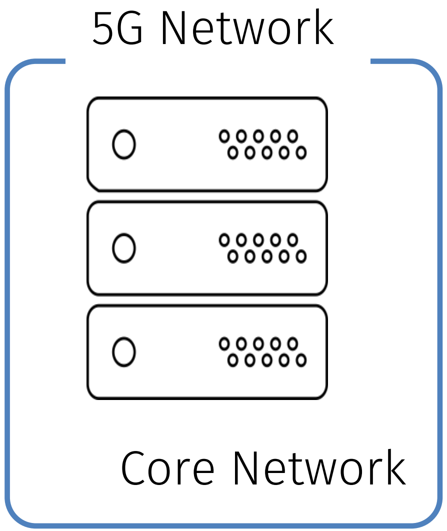
5G SUCI Catchers: Still Catching them all?



5G Smartphone

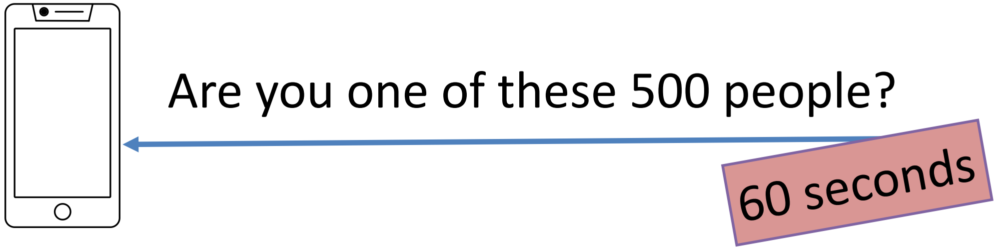


Free5GC + Amarisoft Base Station



Amarisoft Core

1) Validate attack in lab setup ✓
2) Modification to repeat the attack ✓
3) Speed-testing of components ✓
4) Rate-limiting in commercial networks?



	Commercial Networks		
	A	B	C
SIM Speeds	60 / min	300 / min	1000 / min
Network Speeds (Authentication)	36 / min	42 / min	48 / min

Modem Speed: **500 requests/min**

Unthrottled SIM: **780 request/min**

Conclusion on SUPI-Concealment

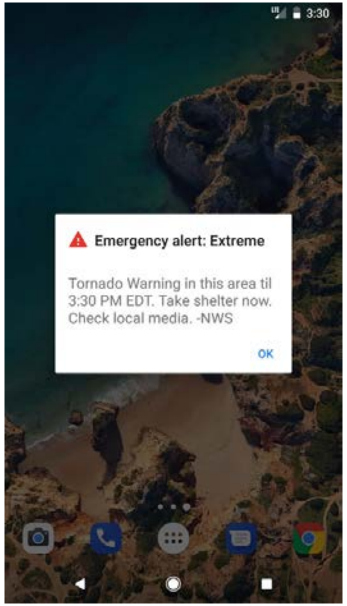
- Commercial networks apply rate limiting and slow down attacks
- SUCI will likely defeat large-scale IMSI-Catchers
- Small-scale user identification can still work
- Operators should deploy SUCI & rate limiting

Evangelos Bitsikas

ACSAC'22
You have been warned: Abusing 5G's Warning & Emergency Systems

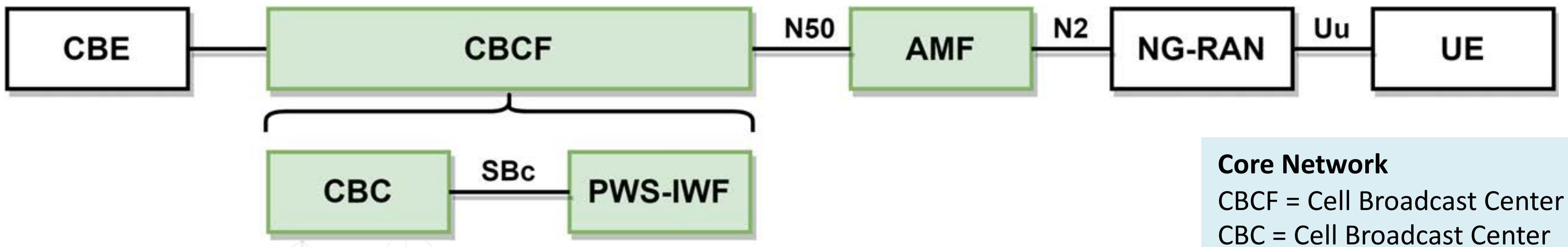
Mobile Network Security

Public Warning System



Public Warning System

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA



STEP 01
Government releases Public Warning Cell Broadcast Message

STEP 02
Alert goes to a Cell Broadcast Entity (CBE)

CBE authenticates originator's credentials and forwards to carriers

STEP 03
Call carrier receives alert at their respective Cell Broadcast Center (CBC) and routes alert to appropriate cell towers

STEP 04
Cell phones within CBC reception area receive alert

Core Network
CBCF = Cell Broadcast Center Function
CBC = Cell Broadcast Center
PWS-IWF = Public Warning System Interworking Function
AMF = Access and Mobility Management Function

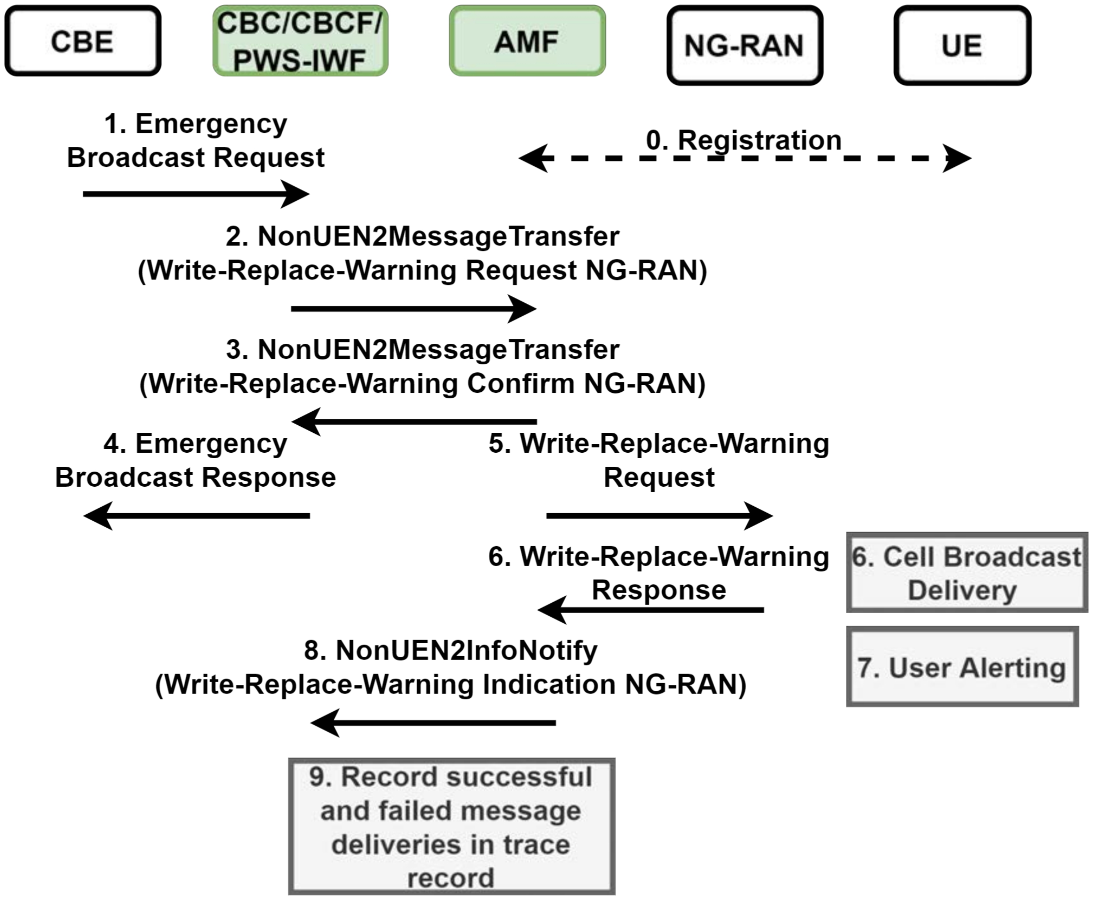
External Entities
CBE = Cell Broadcast Entity
NG-RAN = Radio Access Network
UE = User Equipment

Malicious interference with PWS may aim at:
- Criminal activities
- Fraud
- Political goals
- Terrorism

→ Risk of disasters and human life loss

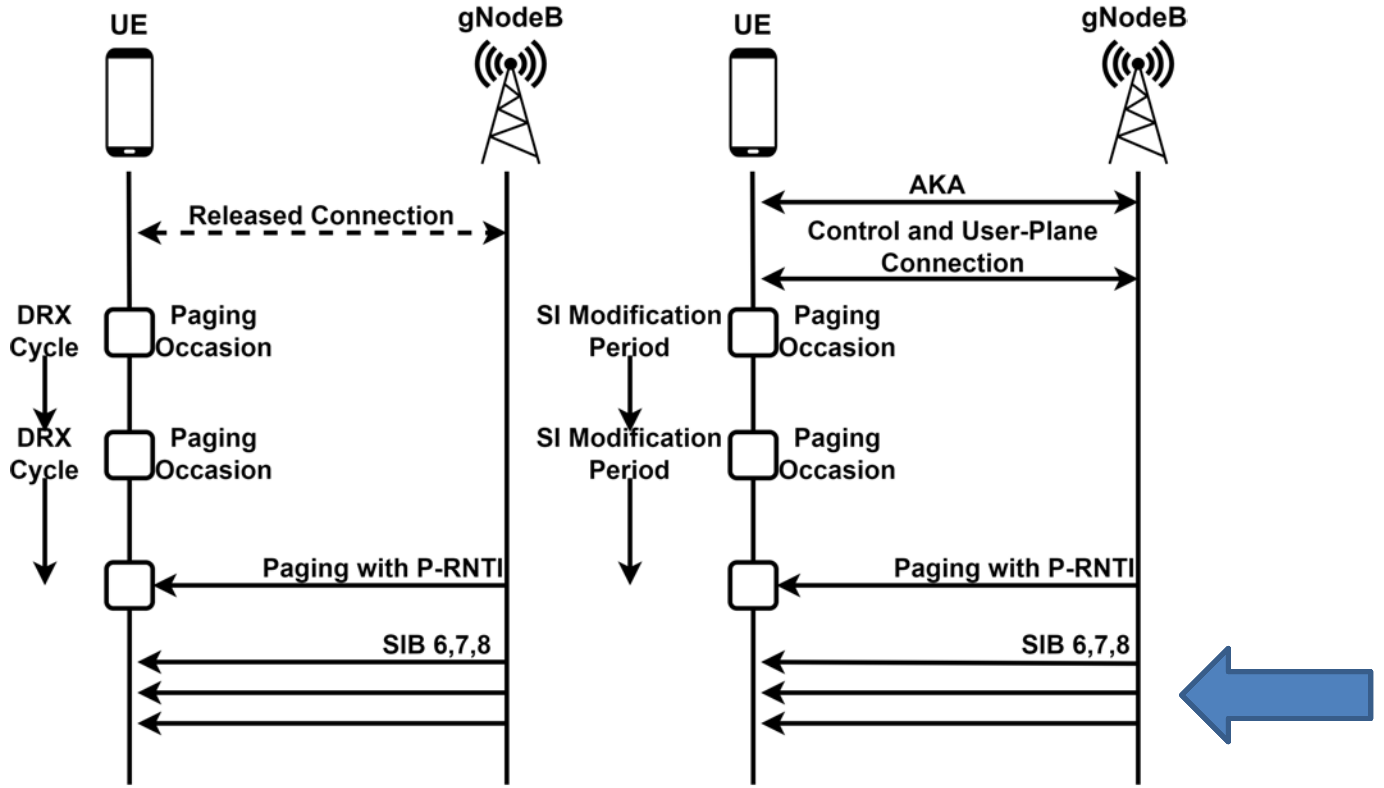
Emergency System

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA



Paging Procedure

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA



Broadcast Transmissions

SIB6 -> *Earthquake and Tsunami Warning System* (ETWS) Primary

SIB7 -> *Earthquake and Tsunami Warning System* (ETWS) Secondary

SIB8 -> *Commercial Mobile Alert System* (CMAS)

Your President is Speaking

- MobiSys 2019

This is Your President Speaking: Spoofing Alerts in 4G LTE Networks

Gyuhong Lee*
University of Colorado Boulder
gyuhong.lee@colorado.edu

Jihoon Lee*
University of Colorado Boulder
jihoon.lee-1@colorado.edu

Jinsung Lee
University of Colorado Boulder
jinsung.lee@colorado.edu

Youngbin Im
University of Colorado Boulder
youngbin.im@colorado.edu

Max Hollingsworth
University of Colorado Boulder
max.hollingsworth@colorado.edu

Eric Wustrow
University of Colorado Boulder
ewust@colorado.edu

Dirk Grunwald
University of Colorado Boulder
dirk.grunwald@colorado.edu

Sangtae Ha
University of Colorado Boulder
sangtae.ha@colorado.edu

ABSTRACT

Modern cell phones are required to receive and display alerts via the Wireless Emergency Alert (WEA) program, under the mandate of the Warning, Alert, and Response Act of 2006. These alerts include AMBER alerts, severe weather alerts, and (unblockable) Presidential Alerts, intended to inform the public of imminent threats.

Recently, a test Presidential Alert was sent to all capable phones in the United States, prompting concerns about how the underlying WEA protocol could be misused or attacked. In this paper, we investigate the details of this system, and develop and demonstrate the first practical spoofing attack on Presidential Alerts, using both commercially available hardware as well as modified open source software.

Our attack can be performed using a commercially-available software defined radio, and our modifications to the open source NextEPC and srsLTE software libraries. We find that with only four malicious portable base stations of a single Watt of transmit power each, almost all of a 50,000-seat stadium can be attacked with a 90% success rate. The true impact of such an attack would of course depend on the density of cell phones in range; fake alerts in crowded cities or stadiums could potentially result in cascades of panic.

Fixing this problem will require a large collaborative effort between carriers, government stakeholders, and cell phone manufacturers. To seed this effort, we also discuss several defenses to address this threat in both the short and long term.

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**; *Spoofing attacks*;

KEYWORDS

Spoofing; Presidential Alert; WEA; CMAS; LTE; Security

ACM Reference Format:
Gyuhong Lee, Jihoon Lee, Jinsung Lee, Youngbin Im, Max Hollingsworth, Eric Wustrow, Dirk Grunwald, and Sangtae Ha. 2019. This is Your President Speaking: Spoofing Alerts in 4G LTE Networks. In *The 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '19), June 17–21, 2019, Seoul, Republic of Korea.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3307334.3326082

1 INTRODUCTION

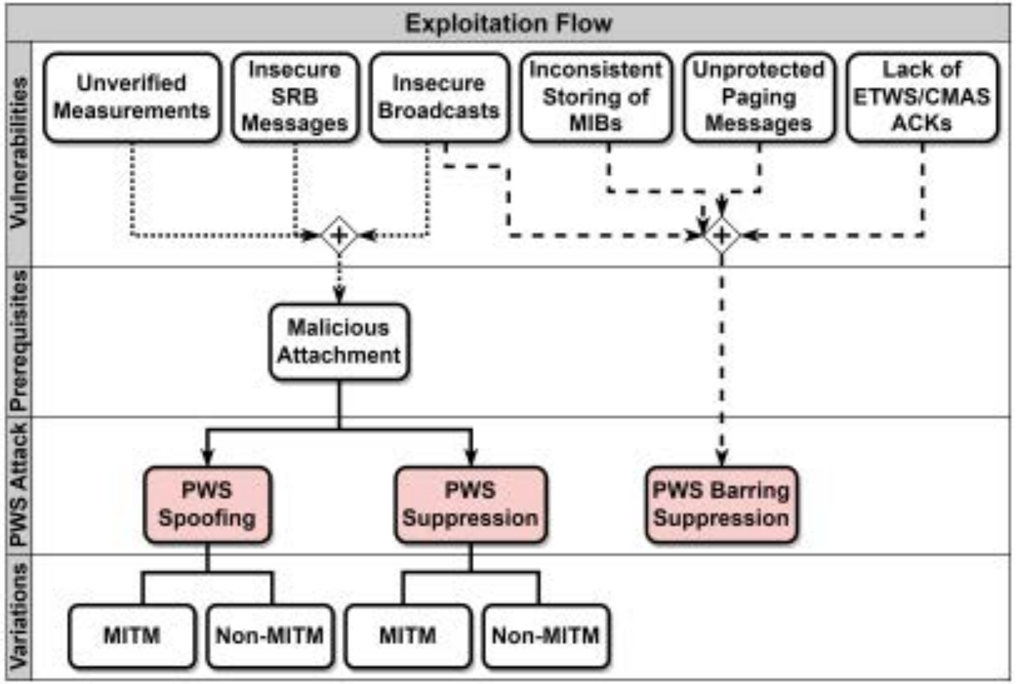
The Wireless Emergency Alerts (WEA) program is a government-mandated service in commercialized cellular networks in the United States. WEA was established by the Federal Communications Commission (FCC) in response to the Warning, Alert, and Response Act of 2006 to allow wireless cellular service providers to send geographically targeted emergency alerts to their subscribers. The Federal Emergency Management Agency (FEMA) is responsible for the implementation and administration of a major component of WEA called the Integrated Public Alert and Warnings System (IPAWS) [47]. IPAWS enables authorized public safety officials to send 90-character, geographically-targeted alerts to the public via

Security Flaws

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

Directly associated:
1. Insecure broadcast messages (SIB 6,7,8)
2. Inconsistent storing of MIB messages
3. Unprotected paging messages
4. Lack of acknowledgements/verifications used in warning system

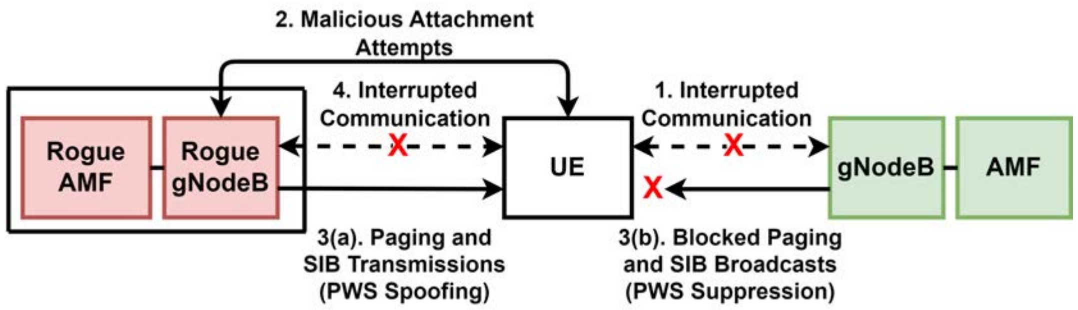
Indirectly associated:
1. Insecure broadcast messages (SIB 1,2,..)
2. Unverified measurements
3. Unprotected Signal Radio Bearer (SRB) messages in RRC

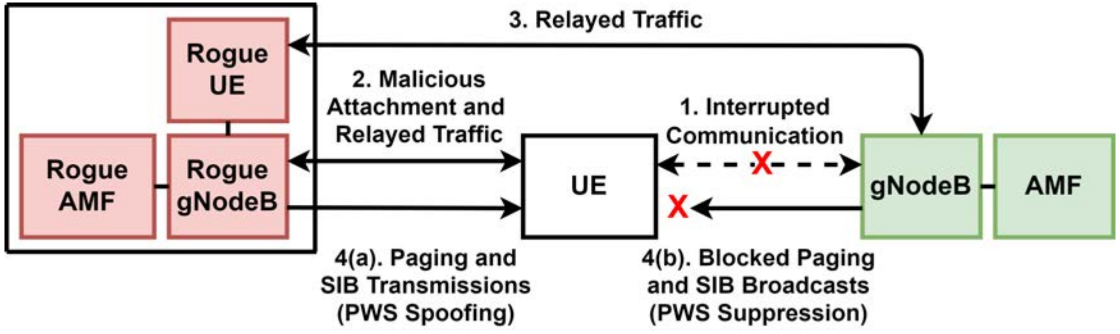


[b] Bitsikas, Pöpper: *Don't hand it over: Vulnerabilities of the handover procedure of cellular telecommunications*. ACSAC 2021

Attacks w/o MitM and w MitM

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA





Spoofing: $D_{spoof}\ (Attach)$

Suppression:

$D_{supp}\ (Attach) \approx D_{spoof}\ (Attach) + t_{rec,supi} + t_{rach,ran}$

D_{spoof} = spoofing time till the UE disconnects
$t_{rec,supi}$ = recovery time of the UE device with a specific SUPI

Spoofing: D_{spoof} (MitM)

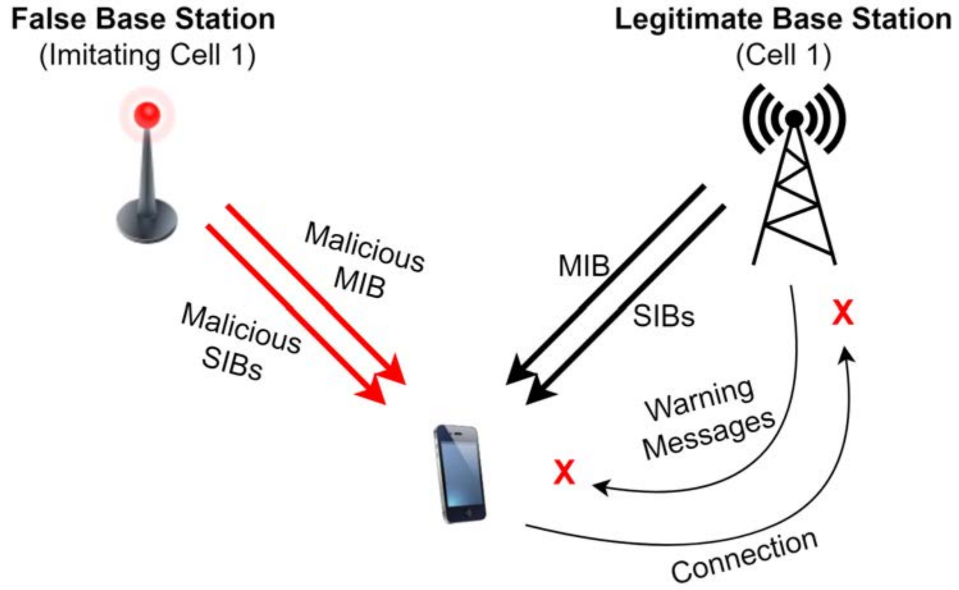
Suppression:

D_{supp} (MitM) $\approx D_{spoof}$ (MitM) $+ t_{rec,supi} + t_{rach,ran}$

$t_{rach,ran}$ = time it takes for the UE to find the legitimate RAN and complete a RACH procedure while beginning the RRC message exchange

Barring Attack

- Disallow any connection to a legitimate base station, thus suppressing the warning messages that are destined for a specific cell/Tracking Area



Requirements:
(1) Set cell_barred of MIB to ’barred’,
(2) intra_freq_reselection of MIB to ’notAllowed’, and
(3) cell_reserved for operator use of SIB 1 to ’reserved’.

Suppression: $D_{supp}\ (Barr) \approx t_{barr} + t_{rec,supi} + t_{rach,ran}$
Signal Strength: $\delta_i \geq 10dB$ (100% success rate)
Limitation: Already active devices may not be affected

Other variation: Overshadowing is also possible

[c] Yang et al.: *Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE*, USENIX Security 2019

Impact

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

PWS Attack	Complexity	Impact	Attack Duration (s)
Spoofing (MitM)	High	High	$D_{spoof}(MitM) \geq 55$
Spoofing (non-MitM)	Medium	Low	$D_{spoof}(Attach) \leq 43$
Suppression by DoS (MitM)	High	Medium	$D_{supp}(MitM) \geq 58$
Suppression by DoS (non-MitM)	Medium	Low	$D_{supp}(Attach) \leq 46$
Suppression by barring	Low	High	$D_{supp}(Barr) \in \mathbb{Q}^{+}$

Spoofing time (MitM): $D_{spoof}(MitM) \geq 55$ sec

Spoofing time (Attach): $D_{spoof}(Attach) \approx 40 - 43$ sec

$D_{spoof}(MitM) > D_{spoof}(Attach)$

$D_{supp}(MitM) > D_{supp}(Attach)$

Responsible Vulnerability Disclosure to GSMA (CVD-2022-0054), FCC, FEMA, CISA & ENISA

Impact

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

FCC Acts to Strengthen the Security of Nation's Alerting Systems

Full Title: Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, et al., PS Docket No. 15-94 et al., Notice of Proposed Rulemaking
Document Type(s): Notice of Proposed Rulemaking
Bureau(s): Public Safety and Homeland Security

Description:
FCC launches a rulemaking to improve the security and reliability of the Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA)

DA/FCC #: FCC-22-82
Docket/RM: 15-94, 15-91, 22-329

Document Dates

Released On: Oct 27, 2022
Adopted On: Oct 27, 2022
Issued On: Oct 27, 2022

Tags:
Cybersecurity - Disaster Response - Emergency Alert System - Emergency Communications - Network Reliability - Wireless Emergency Alerts

Countermeasures

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

Partial PKI-based countermeasure →

- **Signing warning-based SIB broadcasts to avoid spoofing** ✓
- Suppression and barring attacks are still possible ✗
- Replays are possible within a legitimate time frame, but difficult ✗
- Architectural modifications needed ✗

Full PKI-based countermeasure →

- **Signing all MIB and SIB broadcasts could eliminate False Base Stations** ✓
- Eliminates warning attacks ✓
- Replays are possible within a legitimate time frame, but difficult ✗
- Performance overhead and cost ✗
- Architectural modifications needed ✗

Countermeasures

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

Client-based countermeasures →

- **Detection of False Base Stations as mobile applications** ✓
- Restricted practicality (Android phones, rooting, etc.) ✗
- Not a full preventive mechanism against warning attacks ✗
- Adaptive to each network topology ?

Full RRC and NAS protection →

- **Integrity-protection prevents malicious interactions** ✓
- Warning attacks are still possible ✗
- Architectural modifications needed ✗
- Replay protection needed ?

Monitoring and attack detection →

- **Report and verification (measurement reports, MIB/SIB hashes, online sources)** ✓
- Practical with less requirements ✓
- Not a preventive countermeasure ✗

Evangelos Bitsikas

WiSec'23

UE Security Re-loaded: Developing a 5G SA User-Side Security Testing Framework

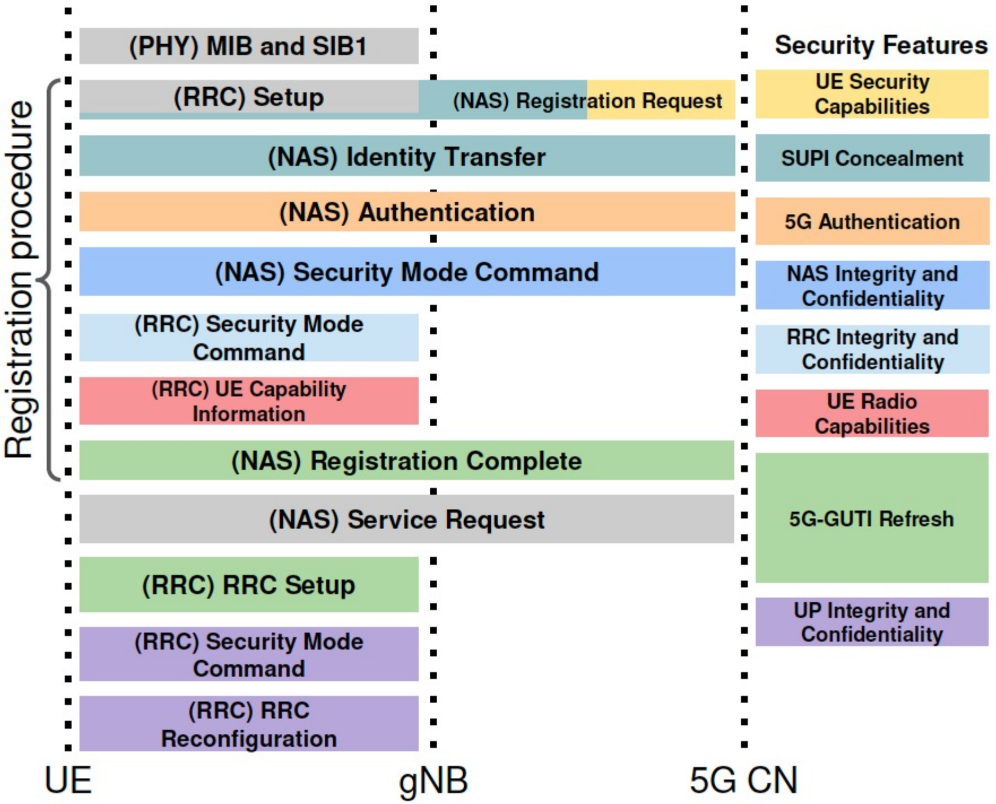
5G Security Testing

Security Testing around the 5G NR Registration Procedure

UE / User-side Testing

WiSec'23

UE Security Re-loaded: Developing a 5G SA User-Side Security Testing Framework



© Oscar Lasierra, Gines Garcia-Aviles, Esteban Municio, Anonio Skarmeta, Xavier Costa-Pérez: European 5G Security In the Wild: Reality versus Expectations. WiSec'23

Network-side Testing

WiSec'23

European 5G Security in the Wild:Reality vs. Expectations

NAS & RRC Testcases

UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework
Evangelos Bitsikas, Syed Khandker, Ahmad Salous, Aanjhan Ranganathan, Roger Piqueras Jover, Christina Pöpper
Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2023

NAS Protocol testcases

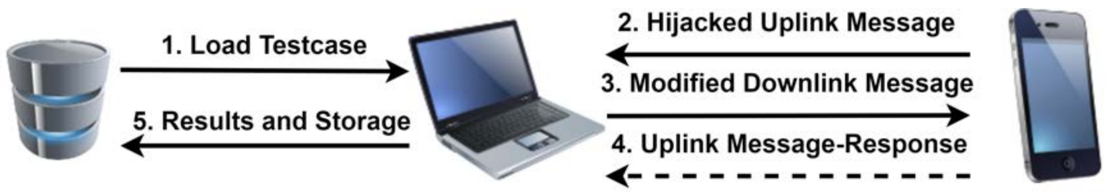
- Null Integrity in Security Mode Command
- Requesting the IMEI before Security Context (Identity Request)
- Ngksi tsc & ksi with 0 value in Security Mode Command
- Modified Replayed Capabilities in Security Mode Command
- Non-zero ABBA value in Security Mode Command
- GMM Cause values (N1 mode not allowed, CAG or authorized for CAG cells only)

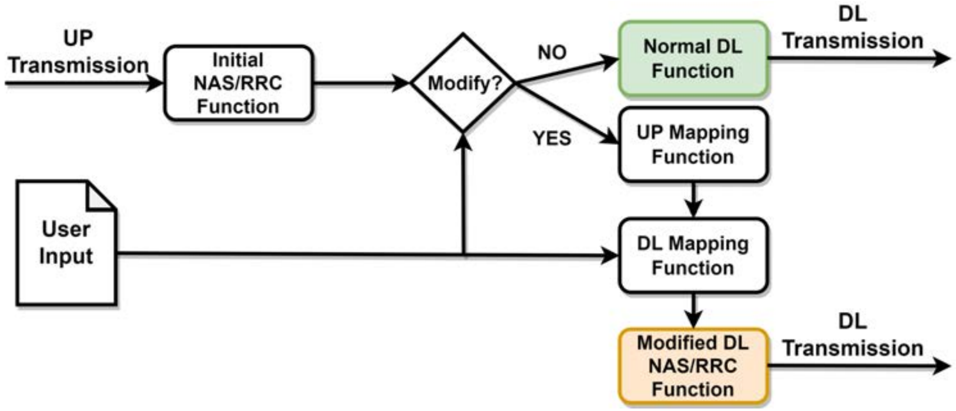
RRC Protocol testcases

- Null integrity in Security Mode Command
- RRCReestablishment before Security Context
- RRCReconfiguration before Security Context
- UE Capability Enquiry before Security Context
- Use of RRCRelease & RRCReject
- RRCCountercheck with invalid msb values

Framework Execution Flow

UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework
Evangelos Bitsikas, Syed Khandker, Ahmad Salous, Aanjhan Ranganathan, Roger Piqueras Jover, Christina Pöpper
Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2023

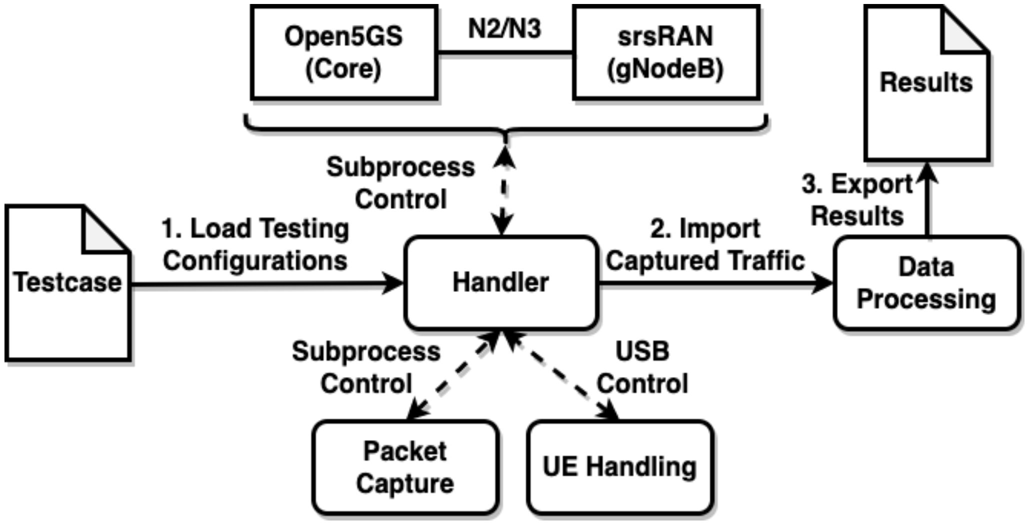




- Modify the NAS and RRC code on UP and DL for control – Hooking approach
- Keep existing functions for normal and unaltered operations
- Create new versions of NAS and RRC functions to include user input
- Introduce testcase logic, format and parsing
- Modify initialization and command control
- Implement device handling and testing automation

Framework Components

UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework
Evangelos Bitsikas, Syed Khandker, Ahmad Salous, Aanjhan Ranganathan, Roger Piqueras Jover, Christina Pöpper
Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2023



UE Handling:

- No rooting required (scrcpy *v2.0*)
- Airplane mode, not rebooting
- iOS manually
- Resetting for every testcase (as for the network)

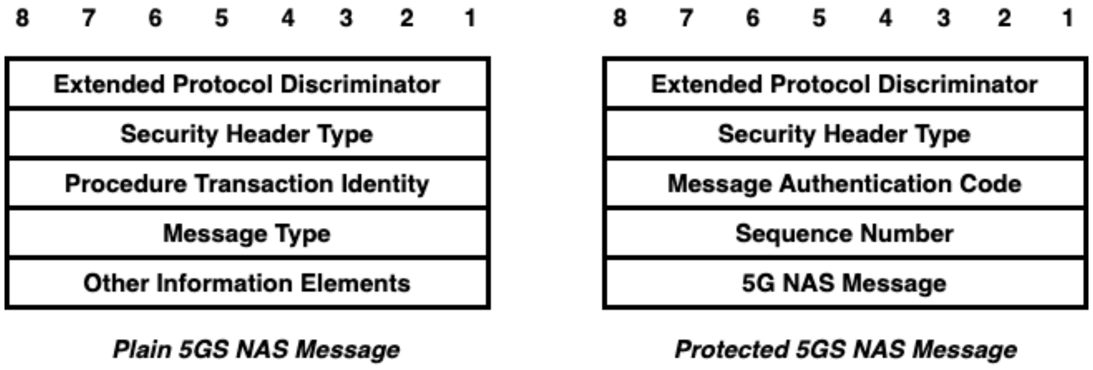
Evaluation Process:

1. Verify that the testcase ran successfully
2. Collect baseband logs
3. Collect the message exchange (pcap)
4. Identify the modified DL message and its response
5. Pass/Fail based on the data and expected behavior

Framework Components

UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework
Evangelos Bitsikas, Syed Khandker, Ahmad Salous, Aanjhan Ranganathan, Roger Piqueras Jover, Christina Pöpper
Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2023


```
[ { //PreAKA
    "ue_ul_handle": "null",
    "dl_reply": "null",
    "command_mode": "null",
    "dl_params": "null"
  },
  { //AKA
    "ue_ul_handle": "security_mode_complete",
    "dl_reply": "registration_reject",
    "command_mode": "send",
    "dl_params":{
      "gmm_cause": "PLMN_NOT_ALLOWED"
    }
  },
  { //PostAKA
    "ue_ul_handle": "null",
    "dl_reply": "null",
    "command_mode": "null",
    "dl_params": "null"
  } ]
```

Testing Categories:
- Misuse of Normal Messages
- Parameter Violations
- Security Header Mismatches
- Wrongly Accepted Messages After Security Enforcement
- Wrongly Accepted Messages Before Security Enforcement

Experimental Setup

UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework
Evangelos Bitsikas, Syed Khandker, Ahmad Salous, Aanjhan Ranganathan, Roger Piqueras Jover, Christina Pöpper
Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2023

Setup:
1. ThinkPad laptop with Ubuntu and USRP B210
2. Custom 5G-capable SIM card
3. Testing PLMN 00101 (for demonstration only)
4. Generated 10s of unique tests for NAS and RRC
5. Calibration and proper parametrization (e.g., NSSAI, TAI, Frequency band, etc.). Check the recent srsRAN tutorial[2].

Device	Chipset	OS	Model	Release
OnePlus Nord 2 5G	MediaTek Dimensity 1200 5G	Android 11	DN2101	2021
Huawei P40 Pro 5G	Huawei Kirin 990 5G	Android 10	ELS-NX9	2020

Tests with SIM cards set with PLMN=01001

↓

Modems are likely to go into a test/debug mode potentially modifying security operations.

↓

Less accurate results for implementation flaws

[2] https://docs.srsran.com/projects/project/en/latest/tutorials/source/cotsUE/source/index.html

Experimental Setup

UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework
Evangelos Bitsikas, Syed Khandker, Ahmad Salous, Aanjhan Ranganathan, Roger Piqueras Jover, Christina Pöpper
Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2023

Security Testing Categories	**OnePlus Nord 2 5G**	**Huawei P40 Pro 5G**
Misuse of Normal Messages	NAS: ✗, RRC: ✗	NAS: ✗, RRC: ✗
Parameter Violations	NAS: ✓, RRC: √	NAS: ✓, RRC: √
Security Header Mismatches	NAS: ✓, RRC: –	NAS: ✓, RRC: –
Wrongly Accepted Messages After Security Enforcement	NAS: ✓, RRC: –	NAS: ✓, RRC: –
Wrongly Accepted Messages Before Security Enforcement	NAS: ✓, RRC: ✓	NAS: ✓, RRC: ✓

✗= vulnerabilities demonstrated/failed tests, ✓= no vulnerabilities detected/passed tests,
√ = some violation observed/inconclusive tests, – = not tested

- *Redirection to EPC required* and *5GS services not allowed* showed a tendency for downgrades.
- *N1 mode not allowed* can lead to 5GMM-NULL state disabling 5GS services in the UE.
- SUPIs (Null-scheme) may face compatibility issues when devices are forced to connect to a 5G network with older SIM cards.

Challenges & Limitations

UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework
Evangelos Bitsikas, Syed Khandker, Ahmad Salous, Aanjhan Ranganathan, Roger Piqueras Jover, Christina Pöpper
Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2023

Framework-based

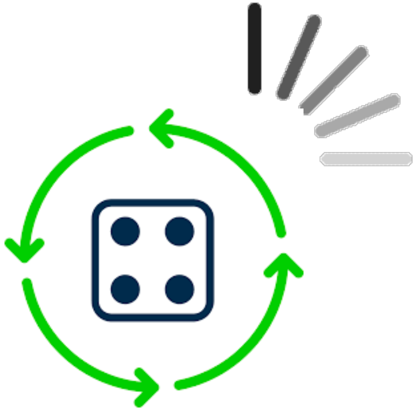
- **Automation of evaluation**: specification analysis issues, uncertain UE behavior.
- **UE Handling**: Issues with iOS devices
- **Limitations of open-source software**: Not fully implemented features, keep up with every update

5G connection-based

- **Correct configuration of 5G setup**: Duplexing division, frequency bands, GPSDO, performance issues (low resources, under-flows, weak signal strength), modulation and coding scheme, etc.
- **PLMN configuration**: Whitelist of PLMNs, 5G capabilities, carrier policies
- **Lack of debugging tools** requires to use Qualcomm Debugger, Network Signal Guru, commercial software and baseband logs. Rooting might be necessary.

Open Research Questions

Open Research Challenges for 5G Security



Security in the Core Network and for Signaling Protocols

- Little public research work

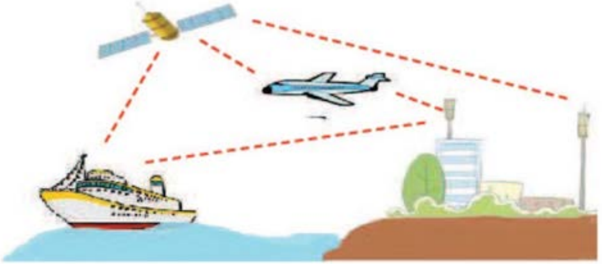
Many Complex Interactions

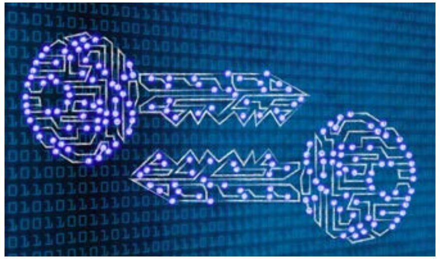
- Bounding attack impact
- Situational awareness, mobility, redundancy/diversity as defense

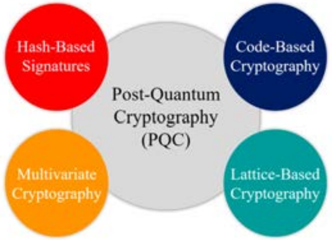
Trust Establishment between Parties

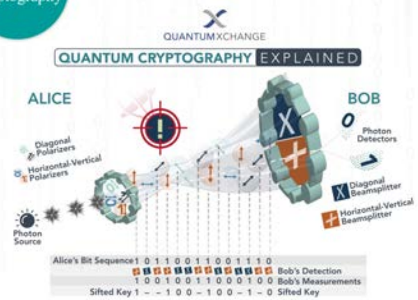
- Unprotected pre-authentication & broadcast messages
- Network functions, cloud services
- Network openness, authentication

Towards 6G Security Research



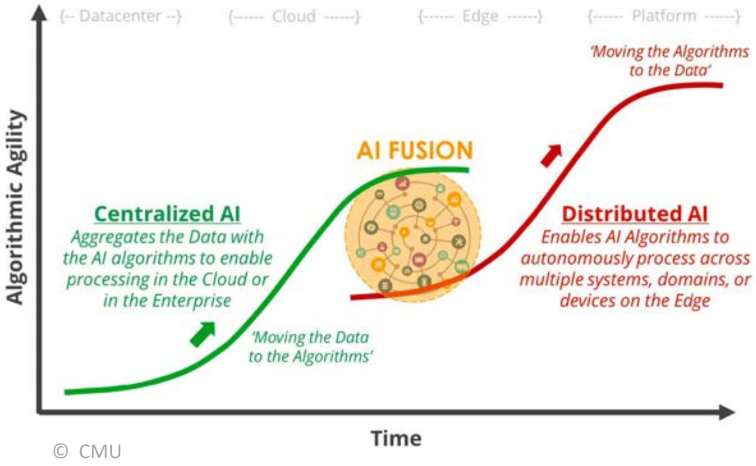






Distributed AI & Intelligent Radios

- Protection against ML attacks: backdoors, injection, model pollution



Global Coverage

- Securely Connecting & Integrating Vertical Applications as diverse as Satellite, UAV, Maritime, Terrestrial
- Not introducing new vulnerabi-lities at their boundaries

Post-Quantum Crypto/Algorithms

- Integration of PQ mechanisms

Conclusion

Why is it great to work on Mobile Network Security

- Real-World International impact
  - For millions of users
- Interesting exchanges / talk invitations with industry
- GSMA, 3GPP, FEMA etc. have standardized processes for vulnerability disclosures
- Many stakeholders and interested researchers
- Funding opportunities

Conclusion

Mobile/Cellular Network Security | Secure Localization & Aviation | Anonymity & Privacy

- Please reach out to me if you'd like to know more or would like to collaborate / get to know more about our work

Thank You for Your Attention!

Christina Pöpper
christina.poepper@nyu.edu
Cyber Security & Privacy Lab (CSP-lab)
https://www.poepper.net