جامعة نيويورك أبوظبي
NYU | ABU DHABI

CSP-lab
Cyber Security and Privacy Lab

CENTER FOR
CYBER SECURITY

NDSS'23 – BoF Session on 5G Security

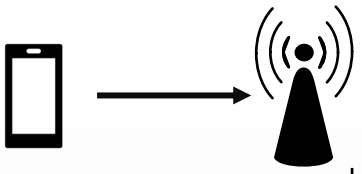
What could possibly go wrong? Experiences with 5G security & privacy and an outlook on 6G

Mar 1, 2023

Christina Pöpper
New York University Abu Dhabi

Security in Cellular Networks – A Quick Pass through the Generations

- Security/privacy issues & vulnerabilities



Our research focus

1G
Audio only w/o security or privacy guarantees
Voice Call/Analog
1980

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

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

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

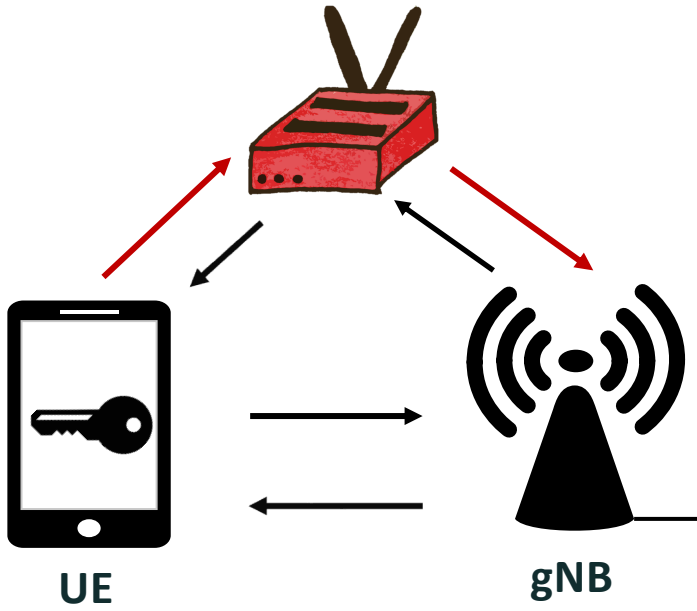
5G
Vulnerabilities in NFV, SDN, and cloud techniques, openness of the network
IoT, VR/AR, Smart City
2020

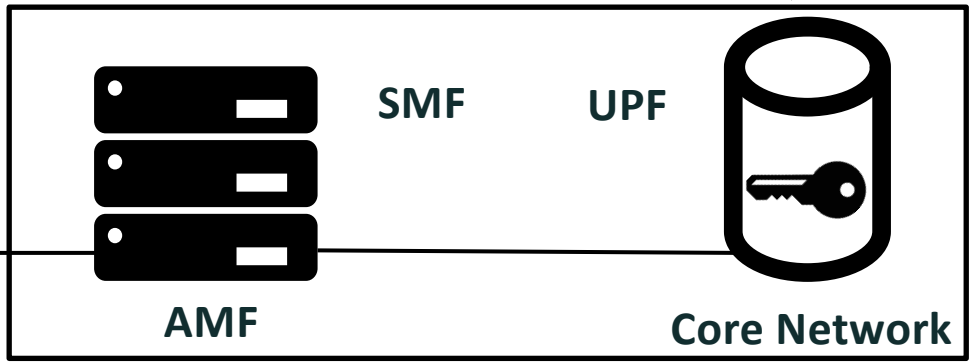
6G
?
Security issues in AI-powered technology, intelligent radios, quantum attacks
Autonomous systems, Multi-sensory XR, Wireless brain computer interaction
2030

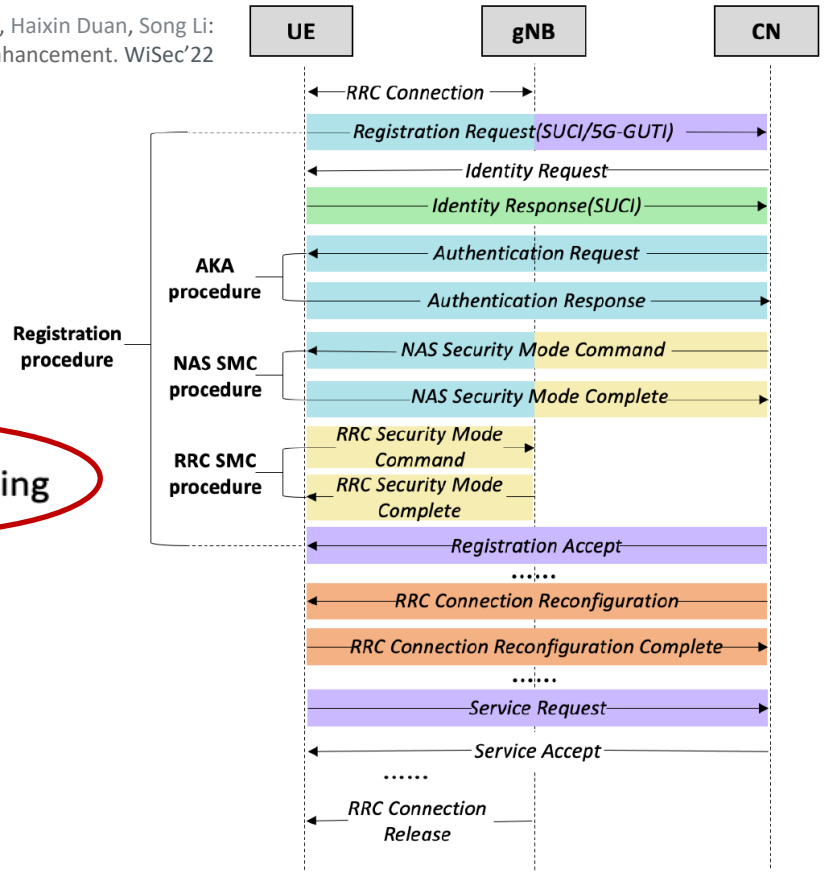
5G Security Features

5G security features:

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



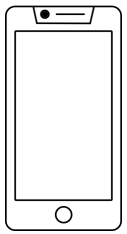




Our Results on 5G Security

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

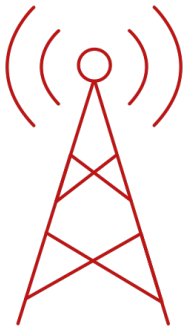
4G IMSI/SUPI Catchers [Fake Base Stations]

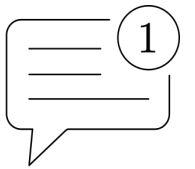


Registration Request

Identity Request

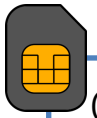
Identity Response: **<SUPI>**





Subscriber <SUPI> was nearby, 12:31

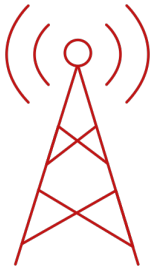
5G SUPI Concealment: SUCI



Operator Public Key + Ephemeral Key + SUPI / IMSI

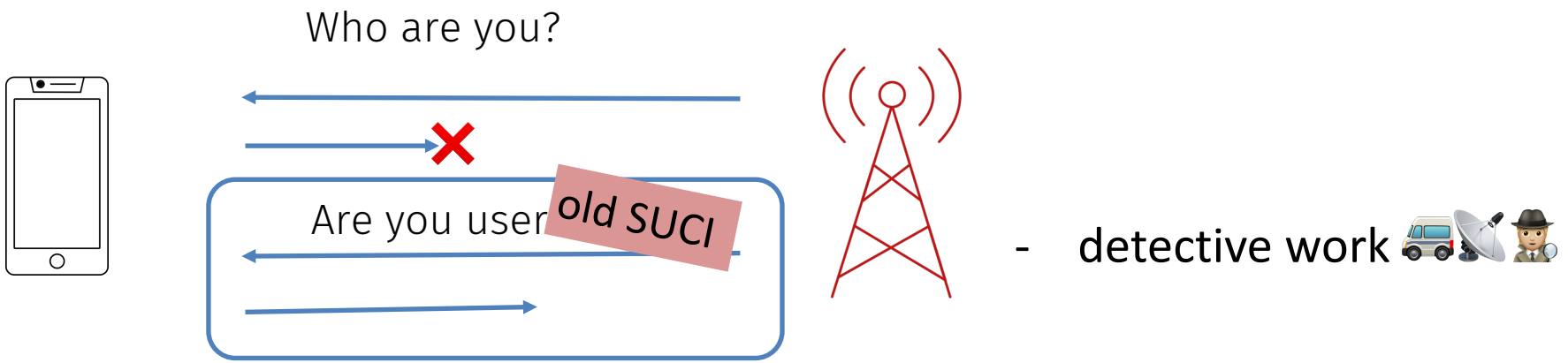
Identity Response: <SUCI, 1>

Identity Response: <SUCI, 2>



same user? can't tell.

SUCI-Catching



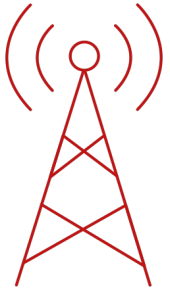
- detective work 🚐📡🕵️

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

Linking SUCIs

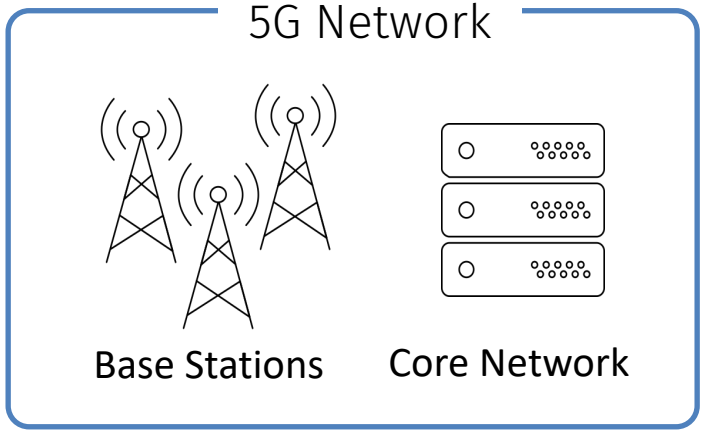
Registration

[new SUCI]



Registration

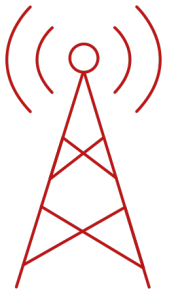
[old SUCI]



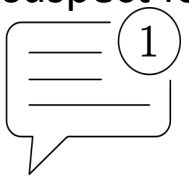
Authentication Request

Authentication Request

unknown subscriber



suspect found



OR

Authentication Failure

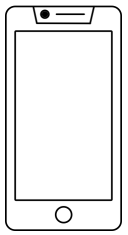
Authentication Response

→ SUCI likely defeats large-scale IMSI-Catchers

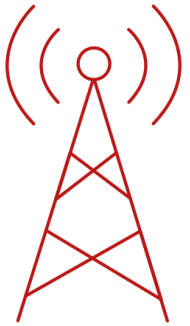
But small-scale user identification still works

5G Experimental Test Setups

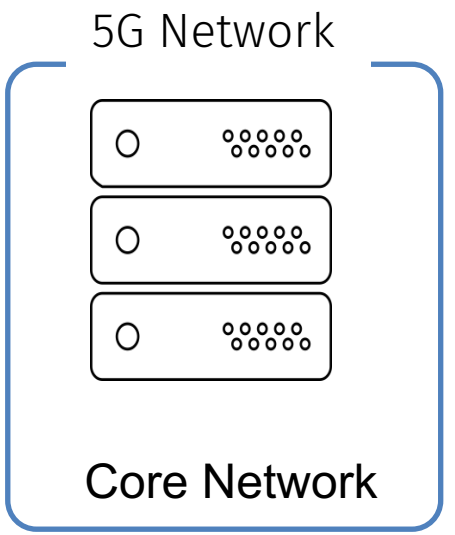
Bitsikas, Pöpper: **Vulnerabilities in the 5G Handover Procedures**, ACSAC, 2021



5G Smartphone

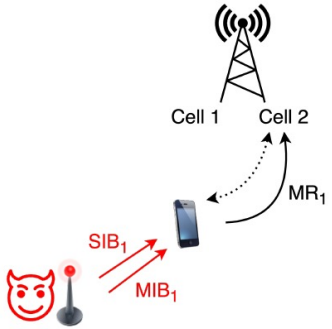


Amarisoft Base Station

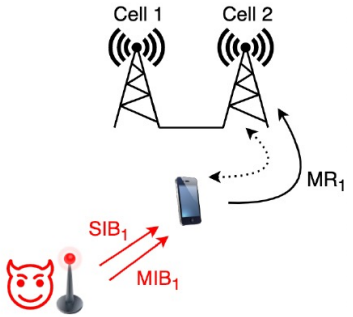


Amarisoft Core

Intra-HO attack case



Inter-HO attack case

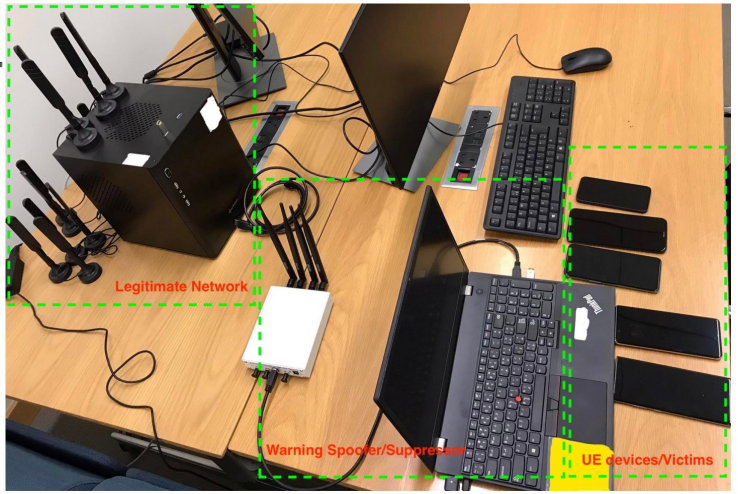


Device	Chipset	OS	Model	Release	MitM Susceptibility	DoS Susceptibility
Huawei P40 Pro 5G	Huawei Kirin 990 5G	Android 10	ELS-NX9	2020	High	High
One Plus 6	Snapdragon 855	Android 10	One Plus A6000	2019	High	High
Samsung Note 10 5G	Snapdragon 845	Android 10	SM-N976Q	2018	Medium	High
Apple iPhone 5	Apple A6 (32 nm)	iOS 10	A1428	2012	Medium	High

Vulnerabilities of the PWS

Bitsikas, Pöpper: **Abusing 5G's Warning and Emergency Systems**, ACSAC, 2022

amarisoft



GSMA: CVD-2022-0054

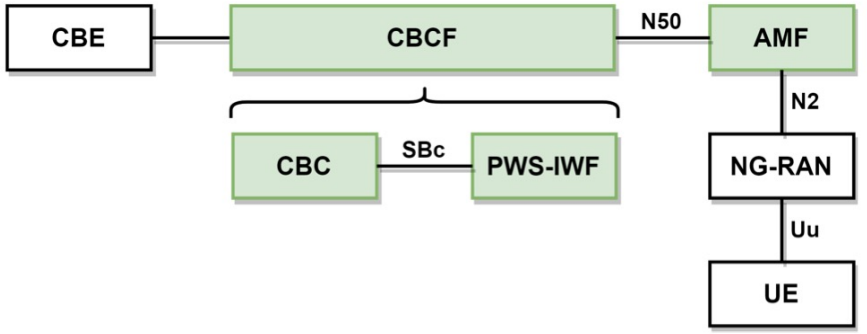
FCC Acts to Strengthen the Security of Nation's Alerting Systems

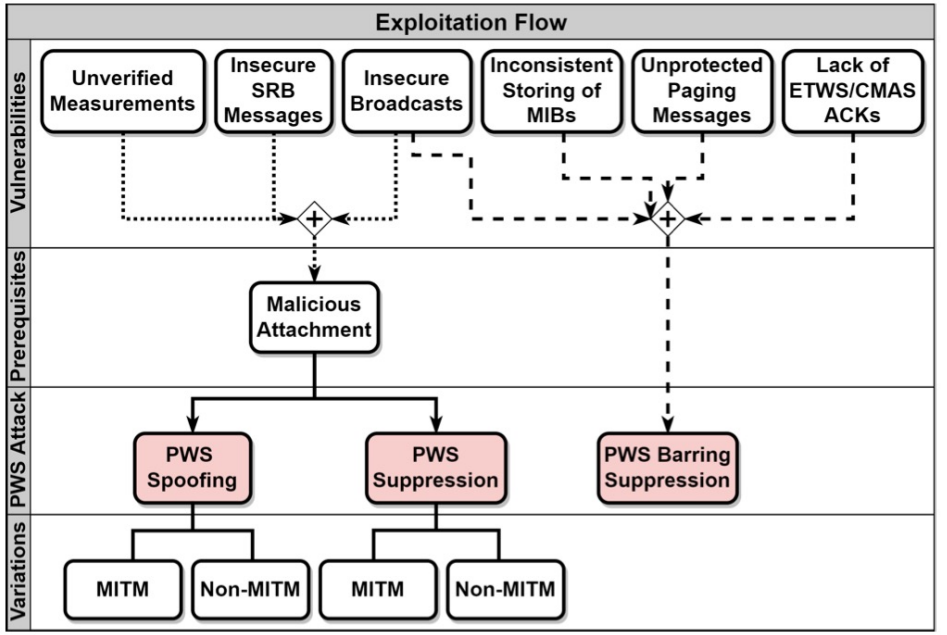
Full Title: Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, et al., PS Docket No. 15-94 et al., Notice of Proposed Rulemaking
Document Type(s): Notice of Proposed Rulemaking
Bureau(s): Public Safety and Homeland Security

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

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

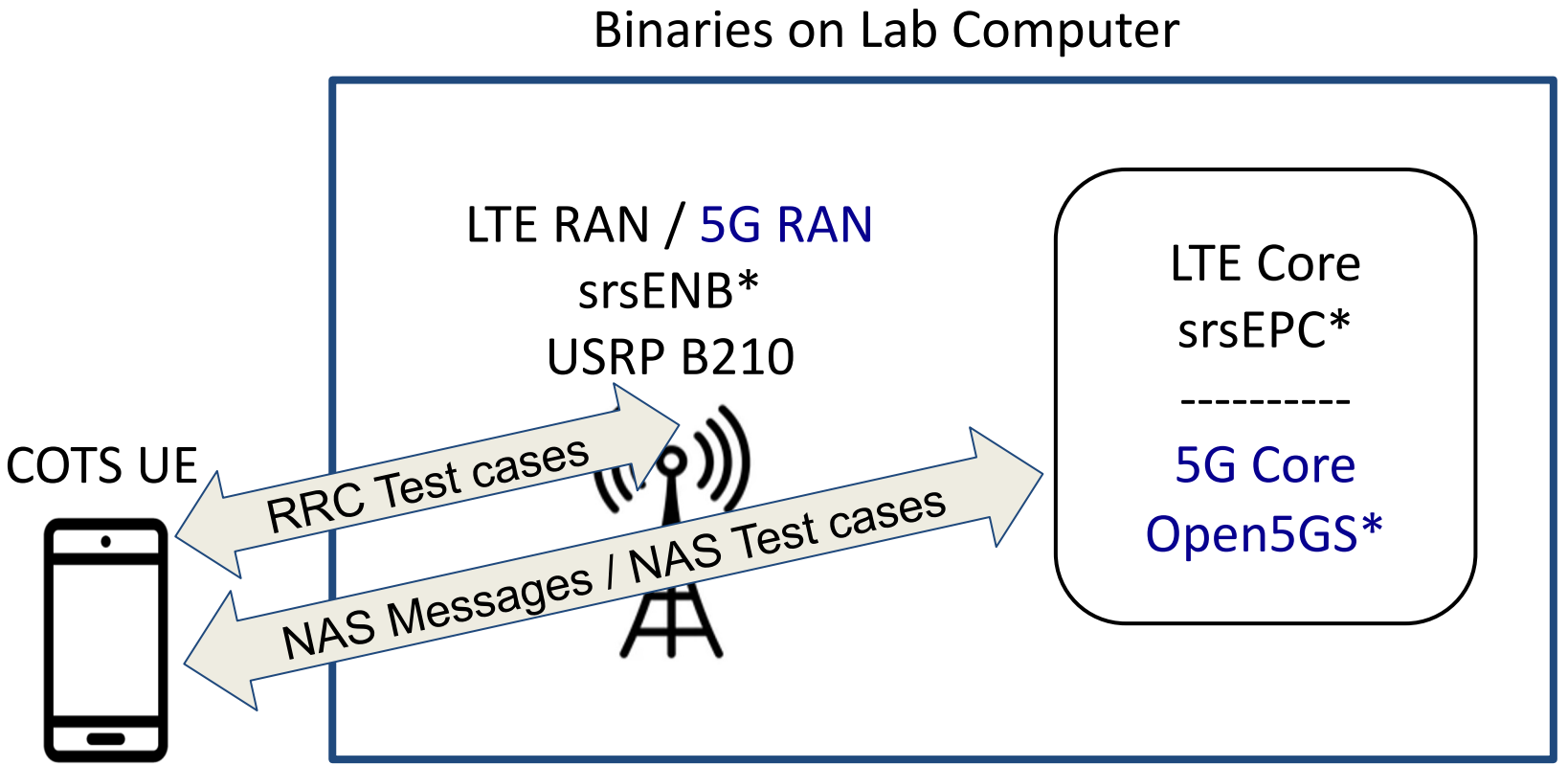
Tags:
Cybersecurity - Disaster Response -



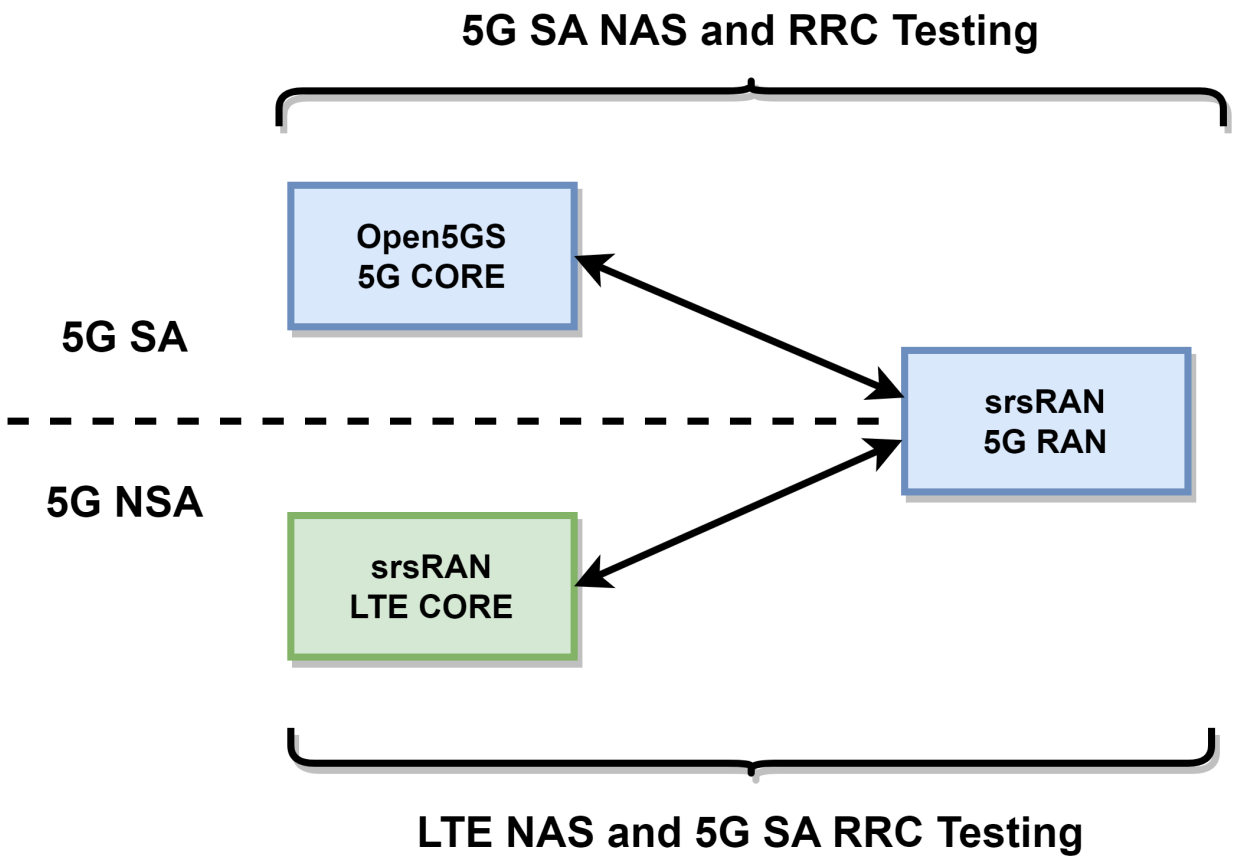


Work in Progress on 5G Security

Work in Progress: 5G UE Security Testing

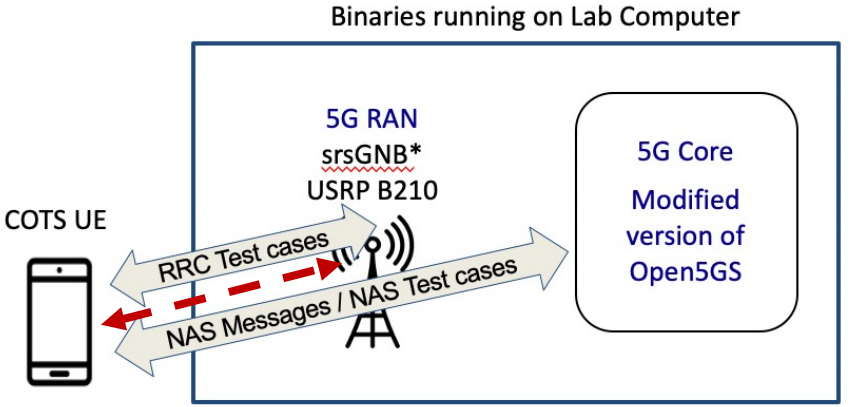


Work in Progress: 5G UE Security Testing



Challenges in Progress: 5G UE Security Testing

- Challenges in establishing (reliable) radio connection from 5G UEs to 5G SA setup
  - Testing of various 5G phones
  - Confirmed connection to AmariSoft CallBox

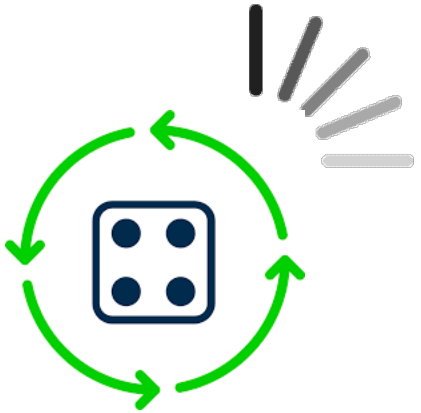


- Issues:
  - UEs do not identify the 5G network, even with manual search
  - Correct configuration files (FDD n3, synchronization, Carrier MCS, etc.)
  - Network carrier policy issue (e.g., whitelisted PLMNs)
  - Lack of debugging tools
  - MAC failures, unknown SUCIs

  → Making step-by-step progress in ruling out causes

Towards 6G Security

Research Challenges for 5G Security



Security in the Core Network and for Signaling Protocols

- Little public research work

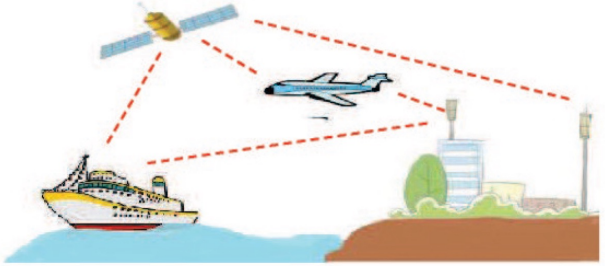
Many Complex Interactions

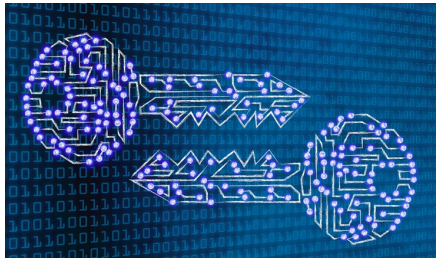
- Bounding attack impact
- Situational awareness, mobility, redundancy/diversity as defense

Trust Establishment between Parties

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

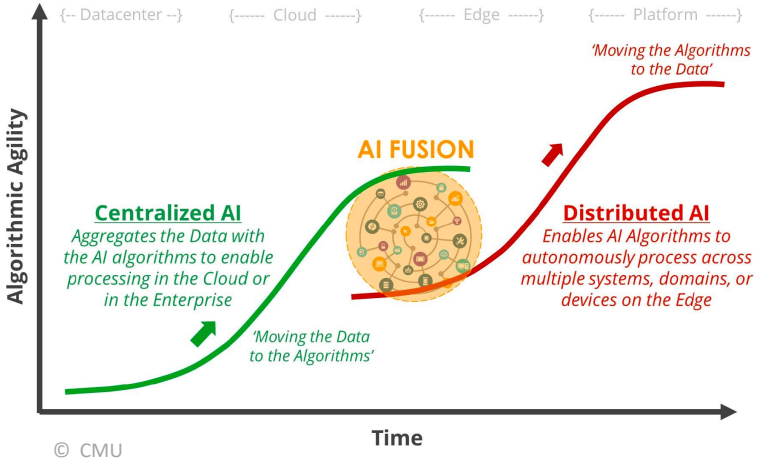
Research Challenges for 6G Security





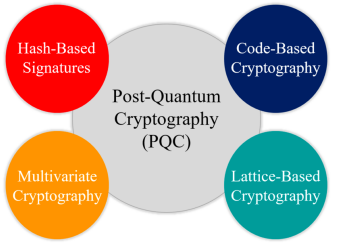
Distributed AI & Intelligent Radios

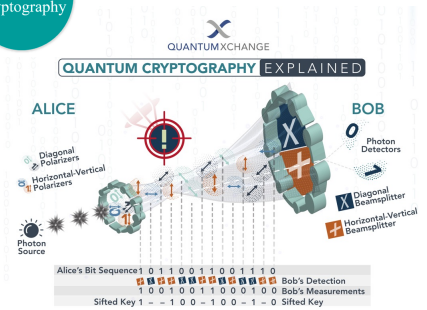
- Protection against ML attacks: backdoors, injection, model pollution



Global Coverage

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





Post-Quantum Crypto/Algorithms

- Integration of PQ mechanisms

Collaborators – Thank You!

Evangelos Bitsikas
@Northeastern U

Syed Khandker
@NYUAD

Ahmad Salous
@NYUAD

Roger Piqueras Jover
@Google

David Rupprecht
@RUB

Merlin Chlosta
@CISPA

Thorsten Holz
@CISPA

Hiring in 5G/nextG Security & Privacy

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