University of Stavanger

Wireless Security (Cellular Networks)

Dr. Ravishankar Borgaonkar

DAT-610

17 Oct 2025

Outline

- Cellular wireless network threats
- Authentication & Encryption in 4G/5G networks
- Security issues in 4G/5G

Concepts used to secure your mobile phone calls and Internet connections!

Is your data transmitted from mobile phone 100% secured?

University of Stavanger

Note : References for the research figure and tables can be found at the last slide number 58.
Some un-referenced pictures are used from Internet to show the subject over online-form of the lecture.

Magic of wireless telecommunication

- First demonstration in 1877 – Stockholm, Sweden
- “Telephone is the instrument of Devil” **
- Innovations - wireline (1877) to wireless (2017)
- Foundation – seamless connectivity and low latency
- Features - quality of service & availability
- Fear and hope

figure- Ericsson History

University of Stavanger

1G Networks – wireless era

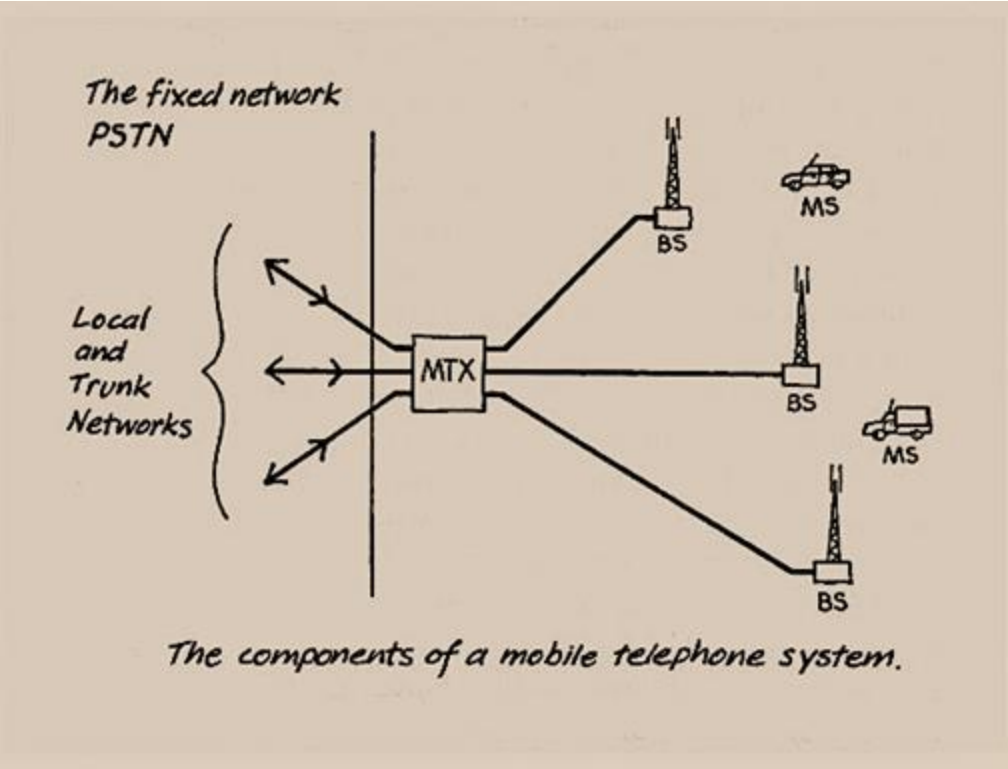


figure- Ericsson History

Problems with 1G

- No authentication & encryption
- Heavy devices
- No roaming – international calls
- But still luxury of talking to loved ones

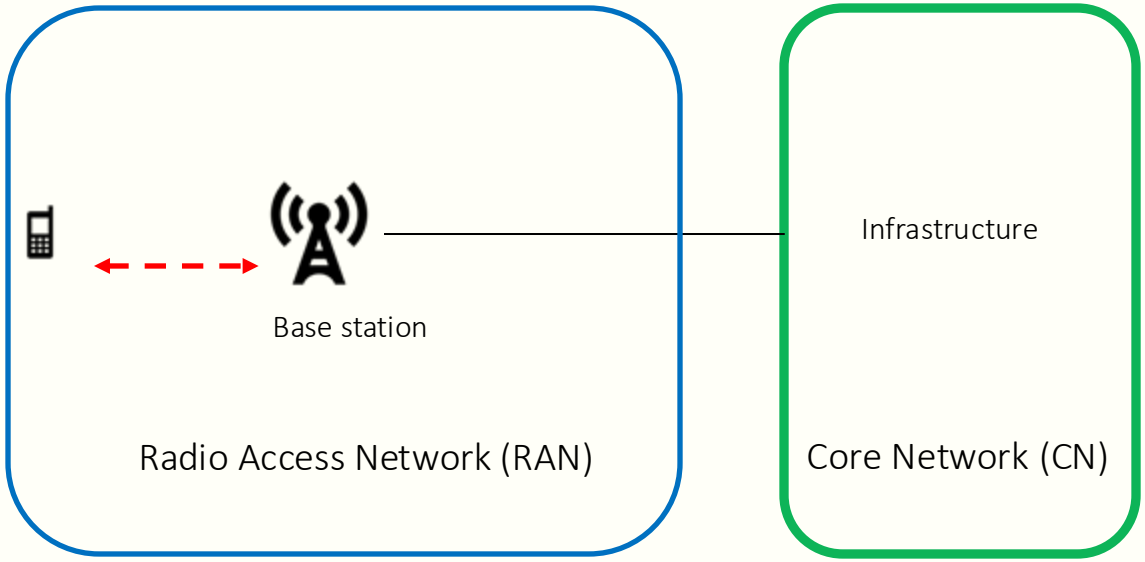
University of Stavanger

Stakeholders & Roles

- Cellular network providers
- End-user equipment vendors
- Standard organizations
- Infrastructure & support services
- OTT services

University of Stavanger

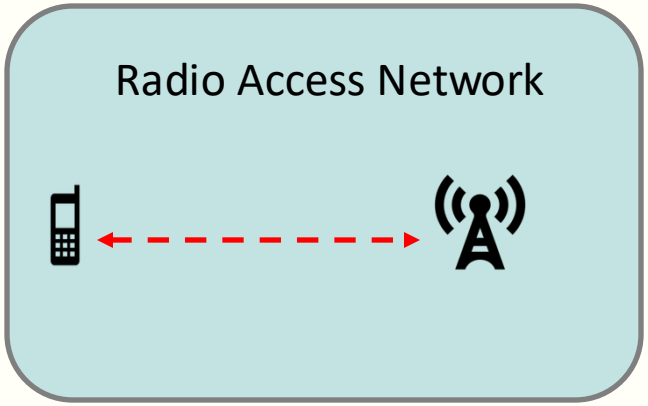
General Cellular Network Architecture



Note: picture provides an abstract view only

Threats to RAN

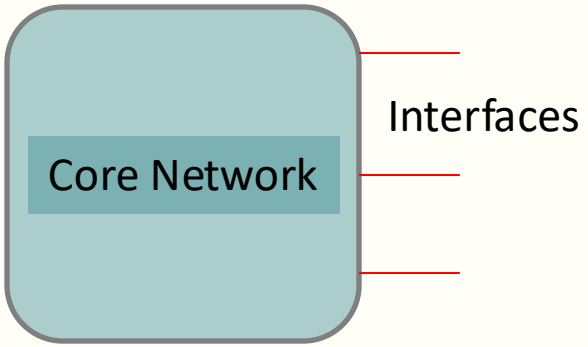
- Interception
- Location tracking
- Man-in-the-middle attacks
- Denial of Service attacks
- Device and identity theft



University of Stavanger

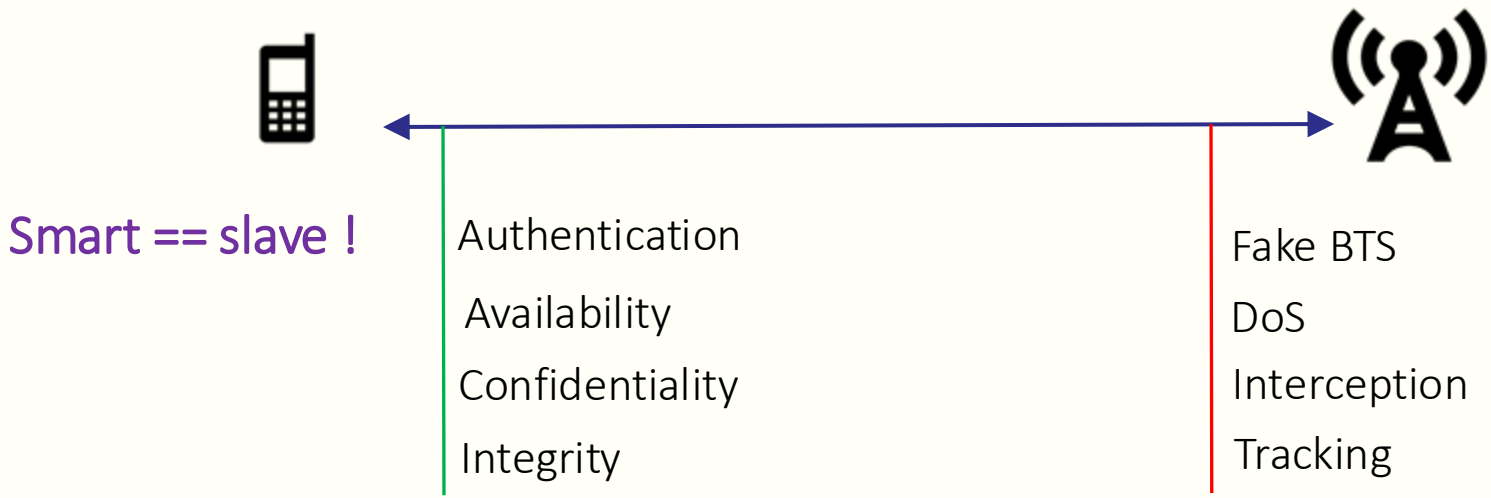
Threats to Core Network

- Espionage
- Insider attacks
- Location tracking
- Billing frauds
- Denial of service



Security aspects

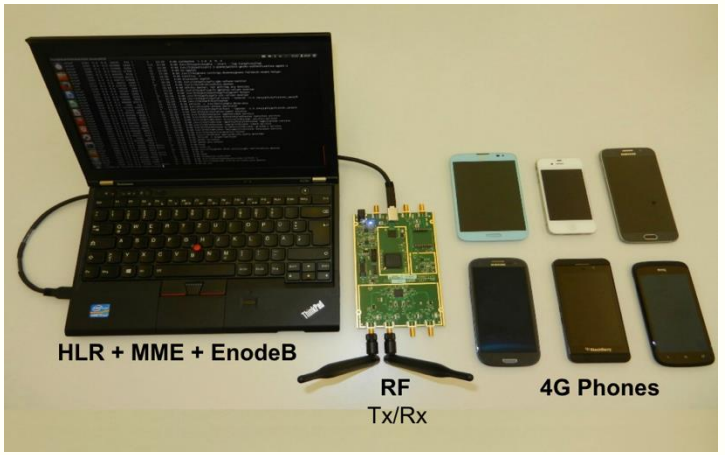
Security aspects & threats



Security tradeoffs play essential role in protocol design!

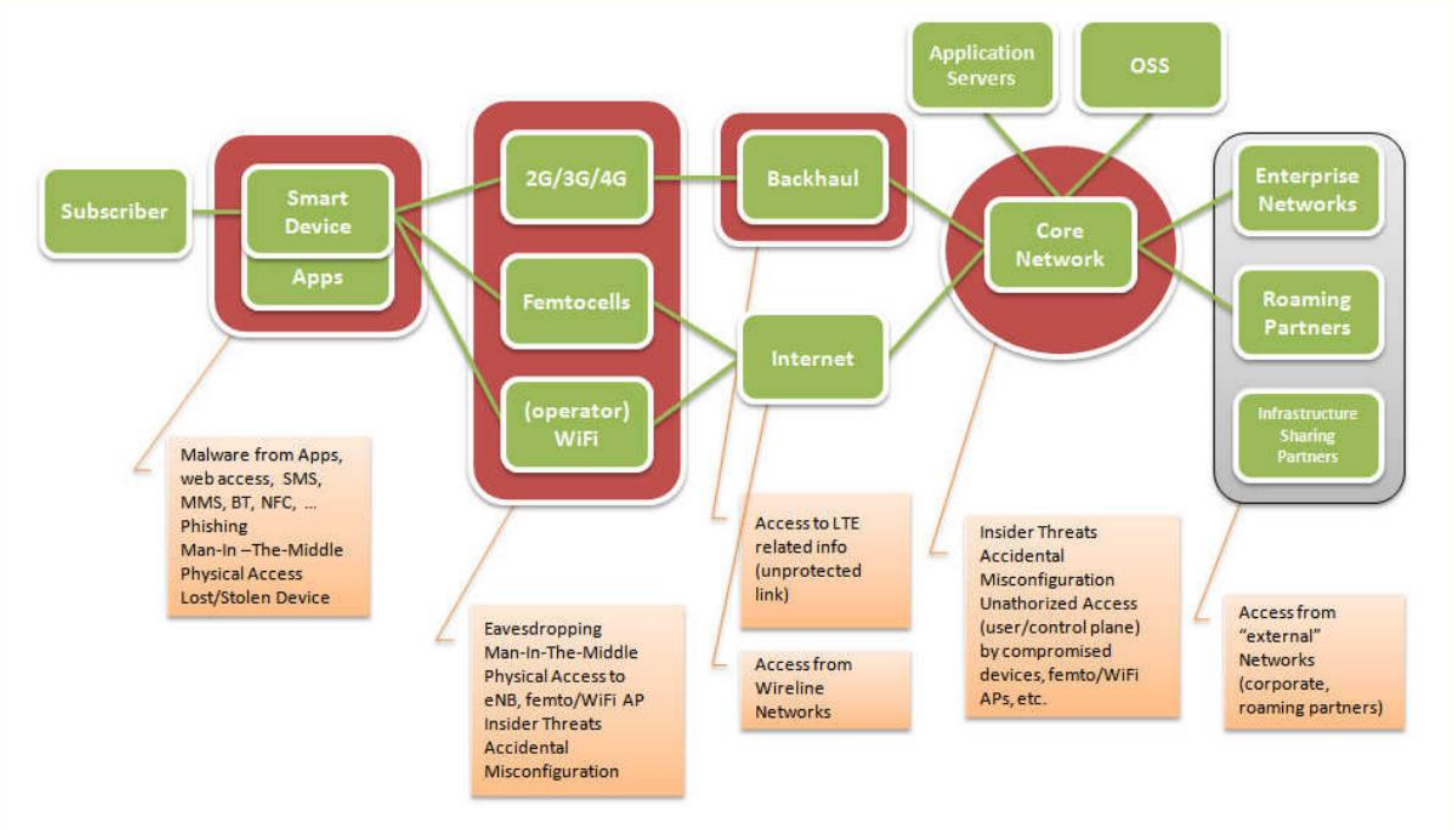
Low cost attacking infrastructure

- 2G/3G/4G* network setup cost < 1000 USD
  - Open source software & hardware
  - USRP, Osmocom, OpenBTS, OpenLTE, etc
- IMSI catcher device problem
- Targeted attacks from illegal actors
- Almost no detection capabilities for the end-users



University of Stavanger

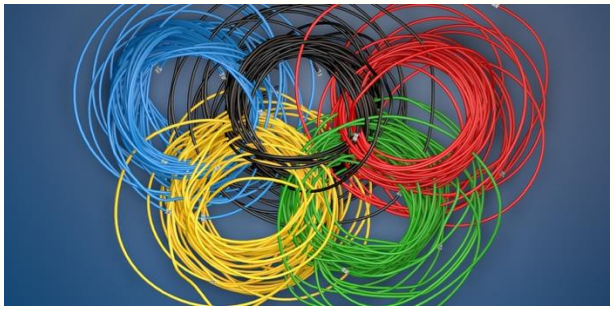
Threat Landscape



University of Stavanger

Attackers

- Fraudsters
- Cyber criminals
- Hackers
- Insider threats
- Cyber warfare actors (arguable)



POSTED BY: TOR INGAR OESTERUD 22. FEBRUARY 2016

Misinterpretation of data from another international operator lead to about 1 million Telenor customers being without mobile coverage for several hours Friday, the company said.

University of Stavanger

Security Principles

- Authentication
  - Symmetric
  - Asymmetric
- Availability
  - Trade-offs
- Integrity
  - Exit points
- Confidentiality
  - Key sizes
  - Choice of encryption algorithms

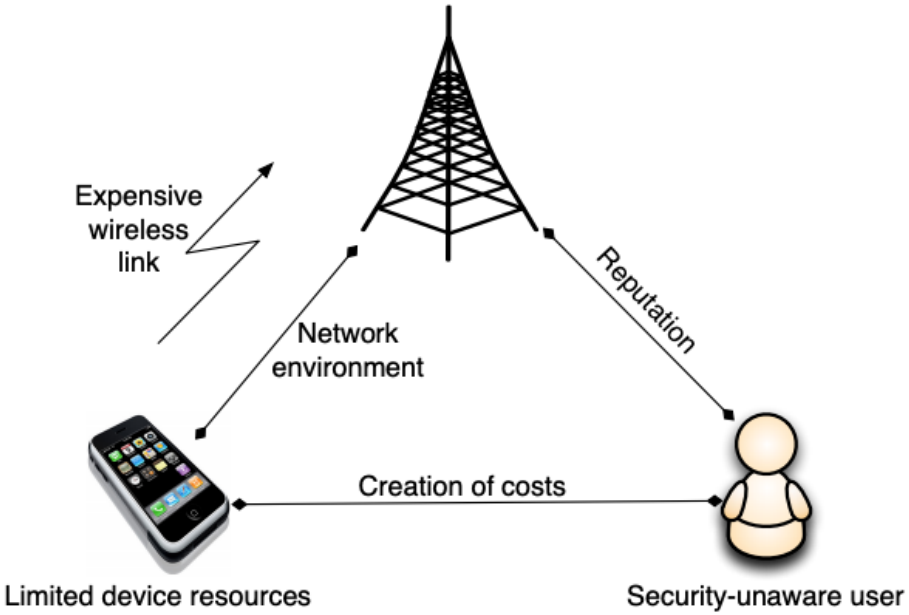


Figure 1. Specifics of Mobile Devices

Transition from 1990 to 2017

- New interfaces – opening up the traditional perimeter
- Low cost hardware/software
- Towards all IP architecture
- backword compatibility – fundamental issues persist
- Increased security level
- Less privacy - daily part of the life!

University of Stavanger

Take Aways

- Complex wireless communication network system
- Network architecture evolved but security add-on
- Necessity of legacy system support
- Many standardized features from 1990 are not necessary in 2017
  - Easy to exploit and not maintained for the updates
- Moore's law principle for open-source development of telco infrastructure

University of Stavanger

Authentication in Cellular Networks

SIM – pillar for authentication

- Subscriber Identity Module

- Universal Integrated Circuit Card (UICC)
  - In GSM, refers as SIM
  - In UMTS system, runs USIM software (entire card is not the USIM)
  - In 4G system, USIM
  - In 5G USIM/eSIM

University of Stavanger

SIM Data (1)

- Integrated Circuit Card ID (ICC-ID) (aka SIM Serial Number - SSN)
  - Uniquely identifies a SIM card (hardware)
- International Mobile Subscriber Identity Module (IMSI)
  - Uniquely identifies the mobile subscriber (15 digits, ITU E.212 standard)
  - MCC (3 digits), MNC (2 or 3 digits), MSIN (9 or 10 digits)
- Authentication Key (K_i)
  - Key shared with provider
  - Never leaves the SIM in any computation
- Authentication algorithms performed on-chip

University of Stavanger

SIM Data (2)

- Location Area Identity (LAI)
  - Stores the last known location area (saves time on power cycle)
- Address book and SMS messages
  - Higher capacity in more advanced cards
  - Have you seen “Inbox full message” in old phones?
- And more …
  - SMSC number
  - Service Provider Name (SPN)
  - Service Dialing Numbers (SDN)
  - value-added-services

University of Stavanger

SIM Application Toolkit

- Before smart phones became popular, the SIM Application Toolkit (STK) was a popular method of deploying applications on mobile phones
  - Allowed for mobile banking applications (and other value added services) to run off the SIM (no handset hardware/OS dependence)
  - Commonly written in Java (for JavaCard) using predefined commands (applications are menu driven)
  - Send data to remote application using SMS
  - OTA update method were eventually incorporated

Security in SIM cards

- Identity and Access control (IMSI, PIN1/PIN2, PUK code)
- Authentication to network operator (Ki, A3)
- Confidentiality (Kc, A8)
- Anonymity (TMSI)
- SIM application toolkit

University of Stavanger

SIM security issues

SIM Cloning (1998)

- Comp128 algorithm leaked
- Reverse engineered & cryptanalyzed

SIM toolkit attacks

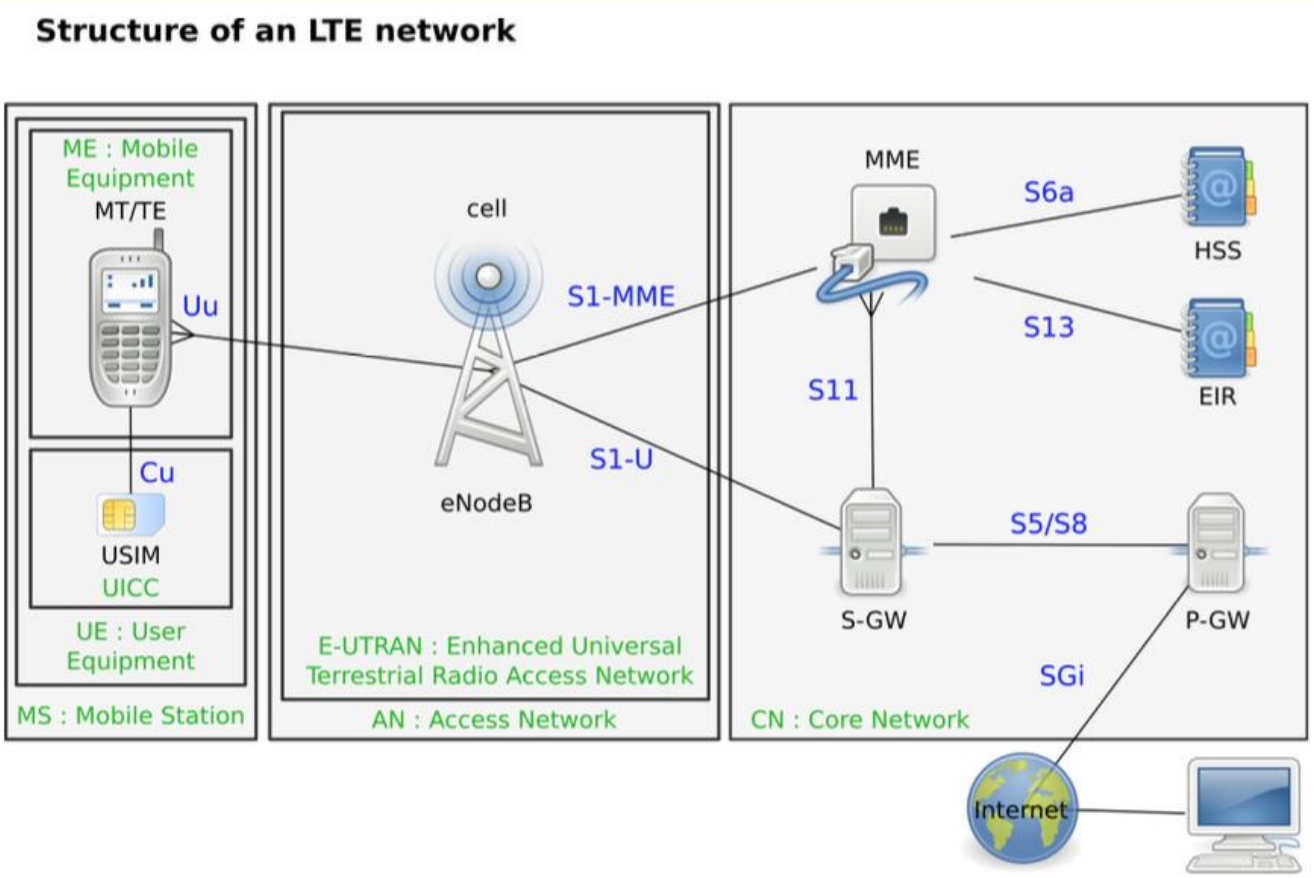
- Fuzzing SMS
- Send premium SMS

Cracking SIM Update keys

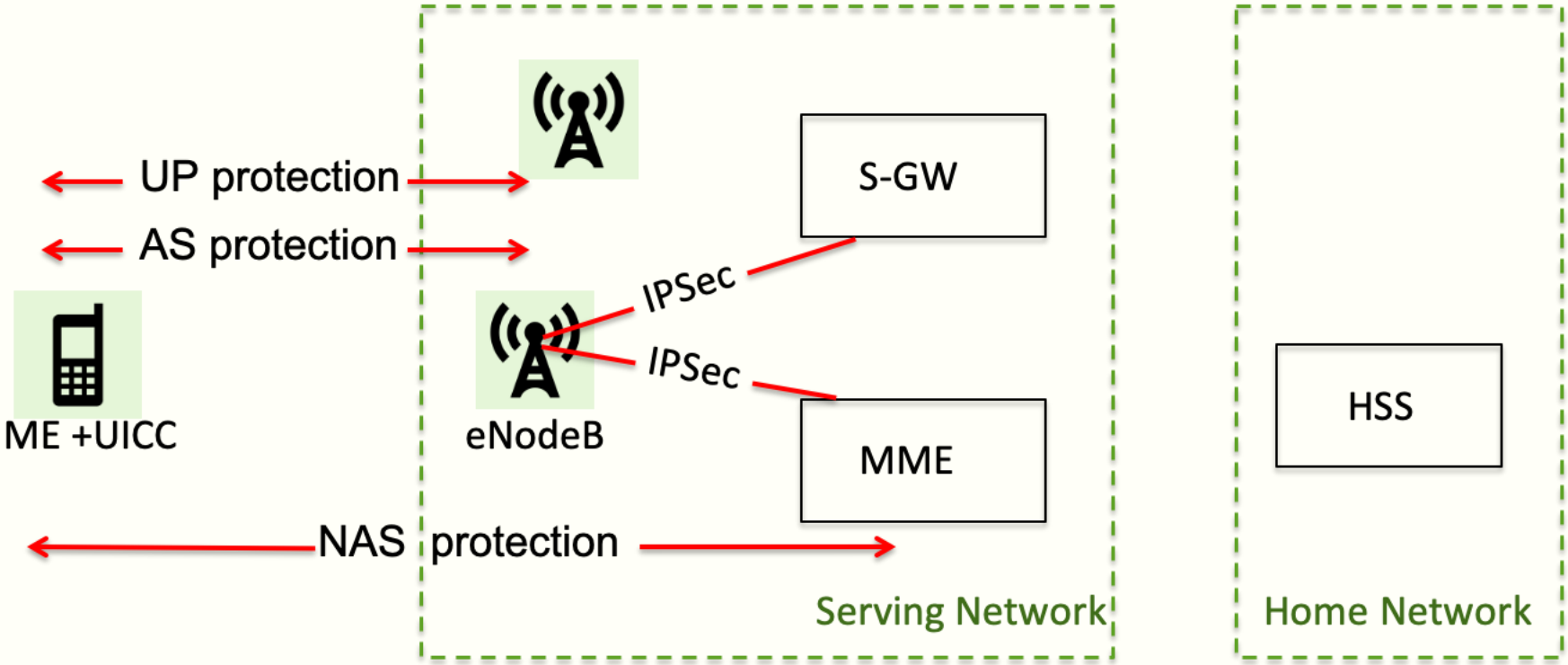
- Recover DES OTA keys
- Singed malicious applets with key

https://www.dn.no/staticprojects/special/2019/mobilkapring/

4G/LTE Network Architecture



4G security architecture

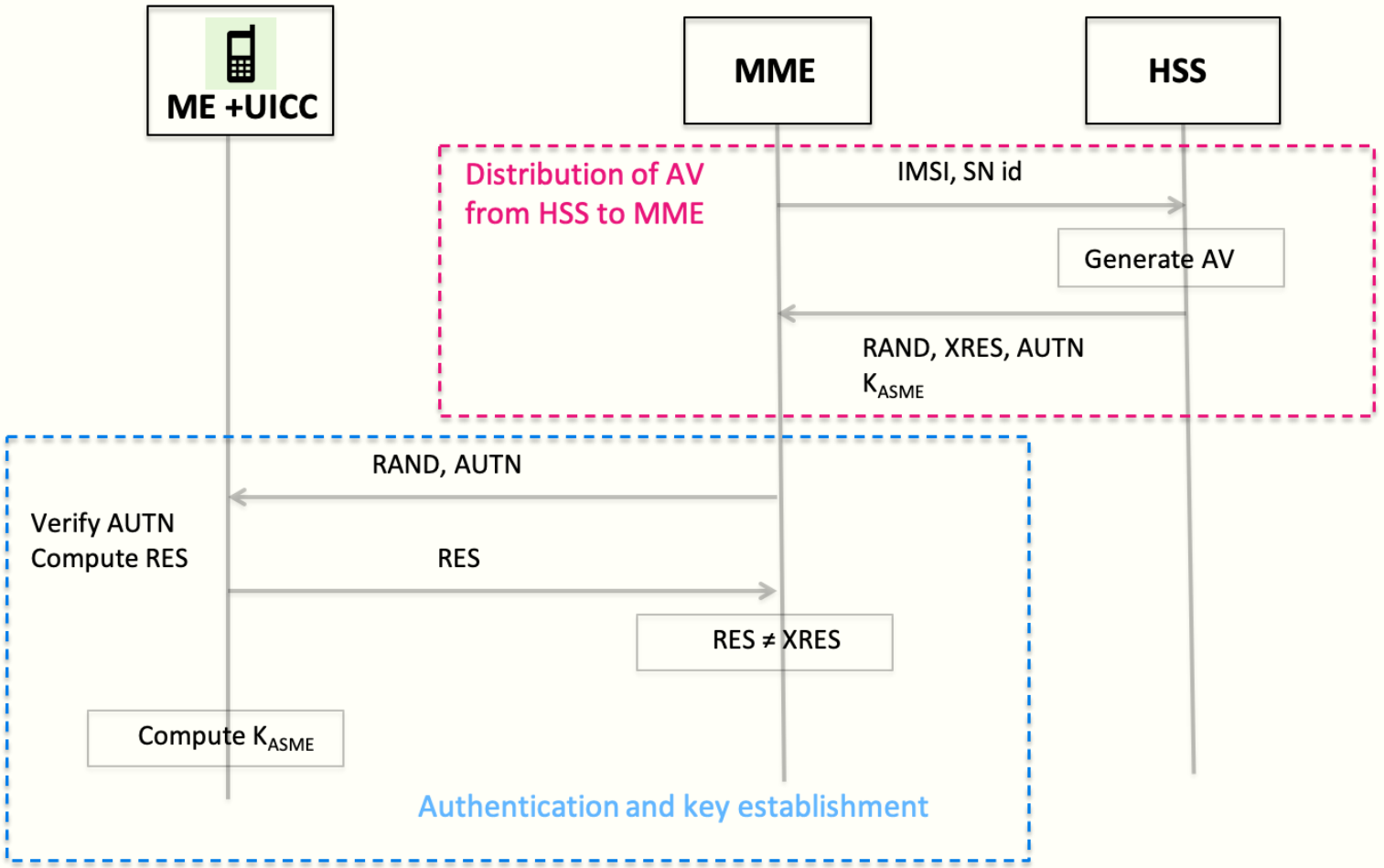


ME Mobile Equipment
UICC Universal Integrated Circuit Card
eNodeB Evolved NodeB
AS Access Stratum
UP User Plane

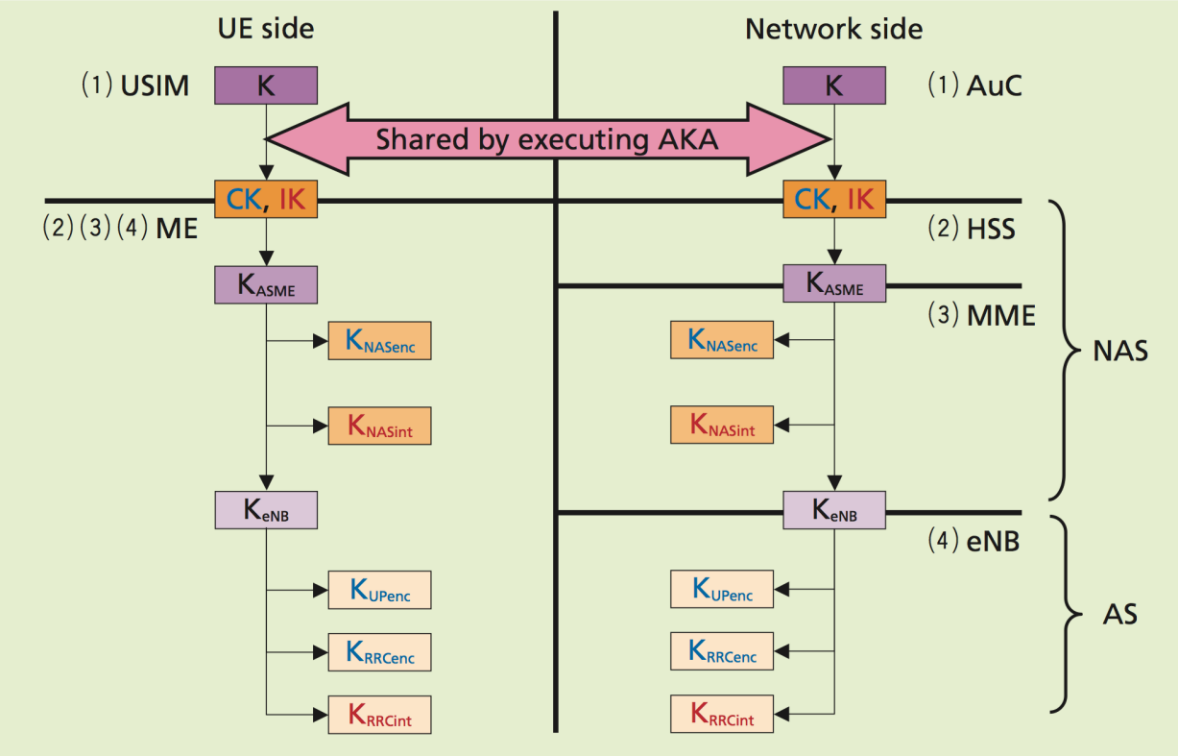
S-GW Security Gateway
MME Mobility Management Entity
HSS Home Subscriber Server
NAS Non Access Stratum

University of Stavanger

4G AKA protocol (simplified)



Key hierarchy



- Cryptographic key separation
- Key renewal
  - Minimize distribution of same key elements
  - Key freshness is important

Source: NTT Docomo Whitepaper

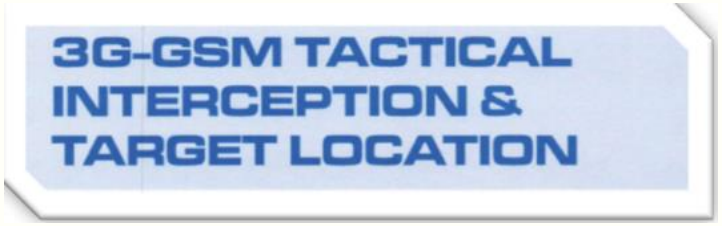
Motivation for Key Hierarchy

- Cryptographic key separation
  - Keys from one context can not be used in other
- Key renewal
  - Minimize distribution of same secret key elements
  - Key freshness is important for secured systems

Emerging attack examples

IMSI catchers (1)

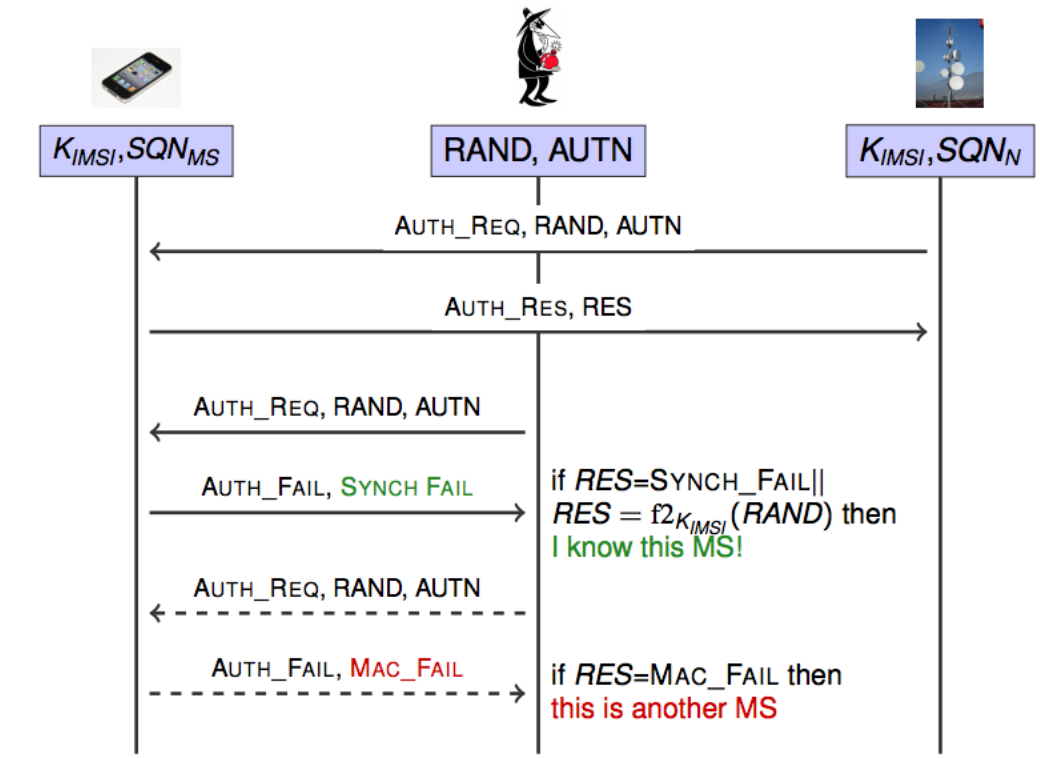
- Exploit weakness in authentication methods
- Location tracking and interception
- Protection for ‘active attacks’ not considered
- Lack of security indicator implementation



University of Stavanger

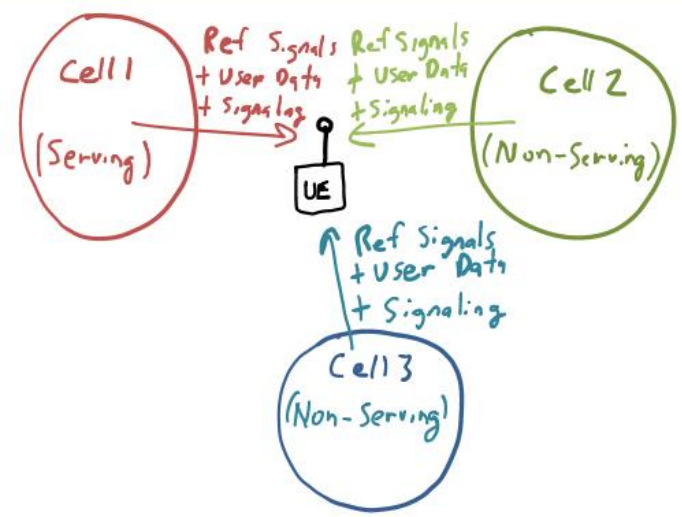
3G/4G AKA vulnerability

- Linkability attack by Arpanis et al
- Affects in 4G as well
- IMSI catcher type attacks



3GPP Specification issues

- RRC protocol – 3GPP TS 36.331
- 'UE Measurement Report' messages
- Necessary for handovers & troubleshooting
- No authentication for messages
- Reports not encrypted



MeasurementReport	+	-	-	Justification for case "P": RAN2 agreed that measurement configuration may be sent prior to security activation

P…Messages that can be sent (unprotected) prior to security activation

A - I…Messages that can be sent without integrity protection after security activation

A - C…Messages that can be sent unciphered after security activation

University of Stavanger

Vulnerabilities in the feature

Specification

UE measurement reports

- Requests not authenticated
- Reports are not encrypted

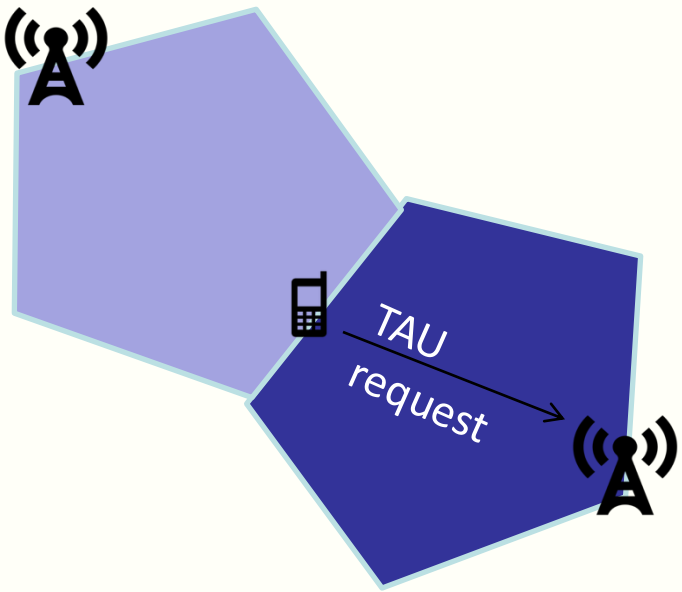
Implementations

RLF reports

- Requests not authenticated
- Reports are not encrypted
- All baseband vendors

4G Feature: Mobility Management

EMM protocol – 3GPP TS 36.331



Tracking Area Update (TAU) procedure

- During TAU, MME & UE agree on network mode (2G/3G/4G)
- "TAU Reject" used to reject some services services (e.g., 4G) to UE

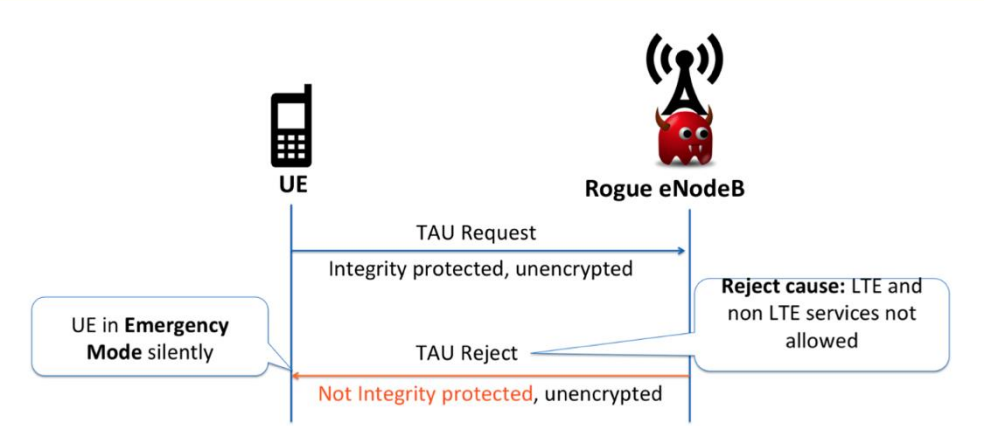
Specification vulnerability: Reject messages are not integrity protected

University of Stavanger

DoS Attacks

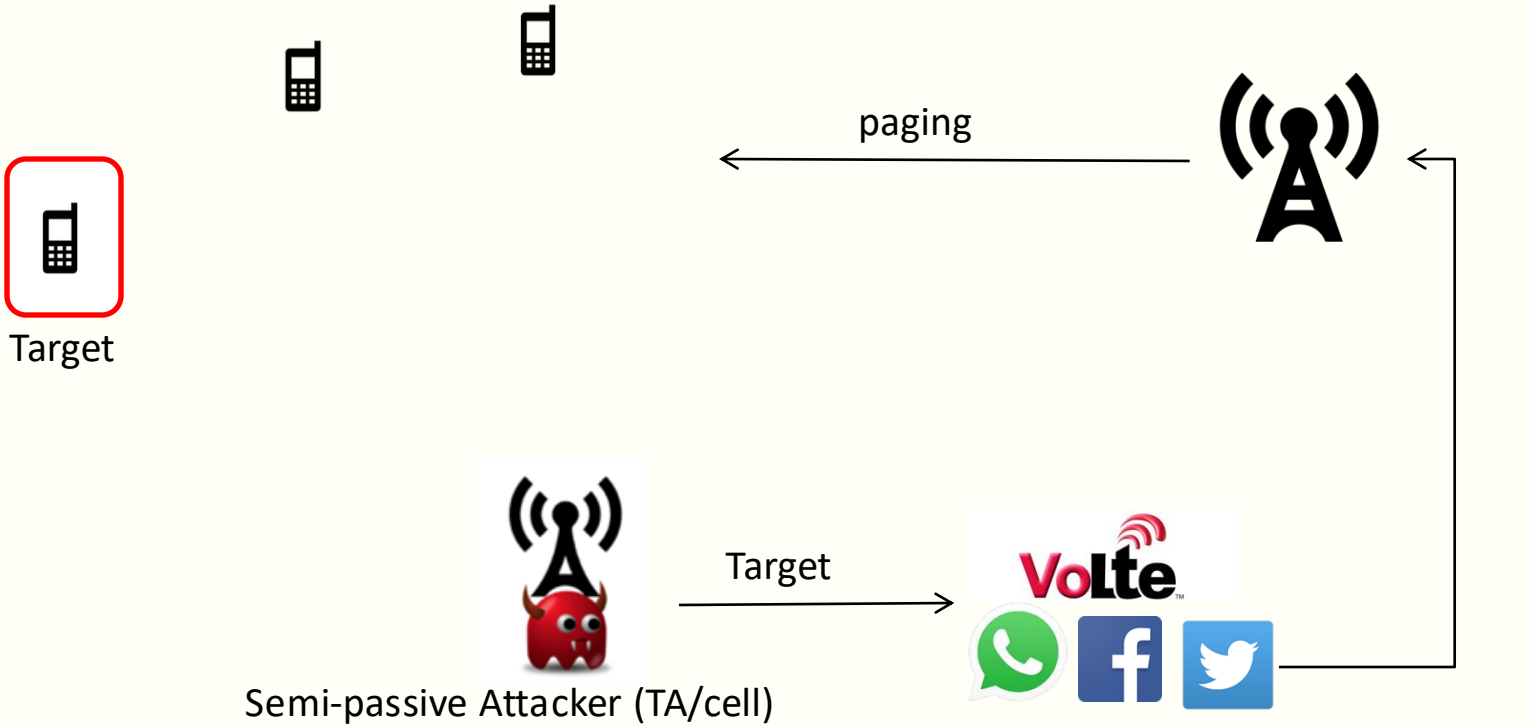
Exploiting specification vulnerability in EMM protocol!

- Downgrade to non-LTE network services (2G/3G)
- Deny all services (2G/3G/4G)
- Deny selected services (block incoming calls)
- Persistent DoS
- Requires reboot/SIM re-insertion



University of Stavanger

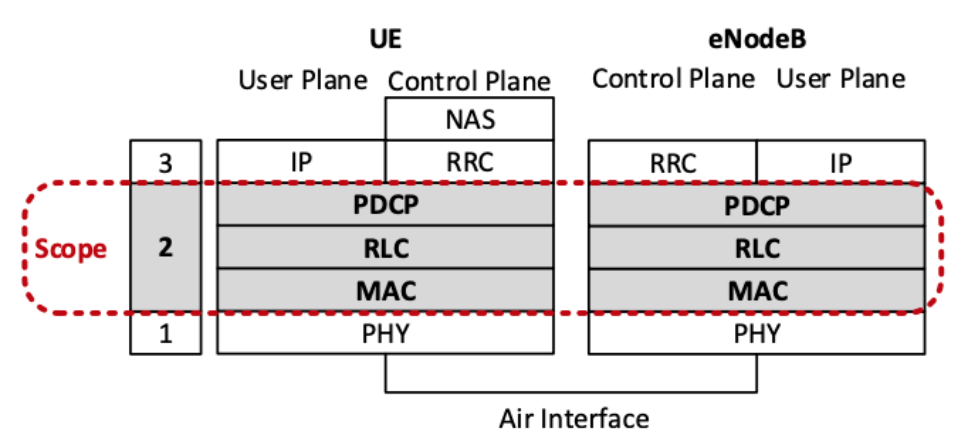
Location Leaks: tracking subscriber coarse level

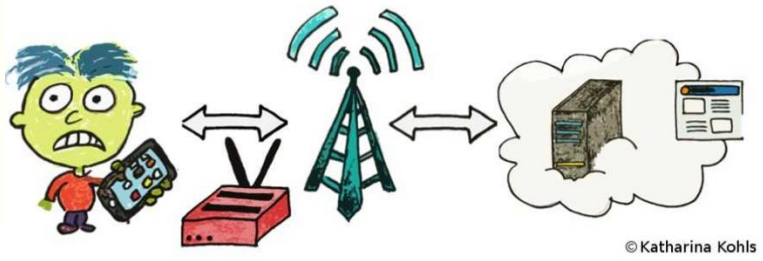


Location Accuracy: 2 Sq. Km

Attacks on Data Link Layer 2

- Passive attacks
  - Identity mapping attack
  - Website Fingerprinting
- Active attack: aLTEr
  - DNS Spoofing attack
  - Man-in-the-middle to intercept communications
  - Redirects to a malicious website

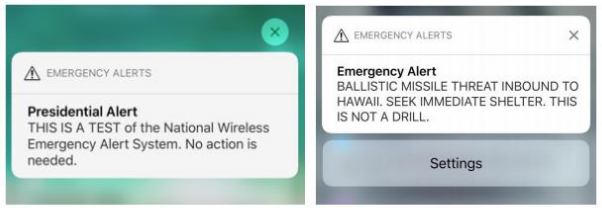




University of Stavanger

SMS spoofing Attacks

- National Alerts
  - Not used in every countries
  - USA – presidential alerts
  - brodcast
- Normal SMS
  - Many tools over Internet
  - But why this is possible?



(a) Presidential alert (b) Imminent threat alert

Figure 1: Snapshots of real WEA alerts received by cell phones: (a) the first national test of the Presidential Alert performed on Oct. 3, 2018 in the US, and (b) a false alert sent in Hawaii on Jan. 13, 2018.

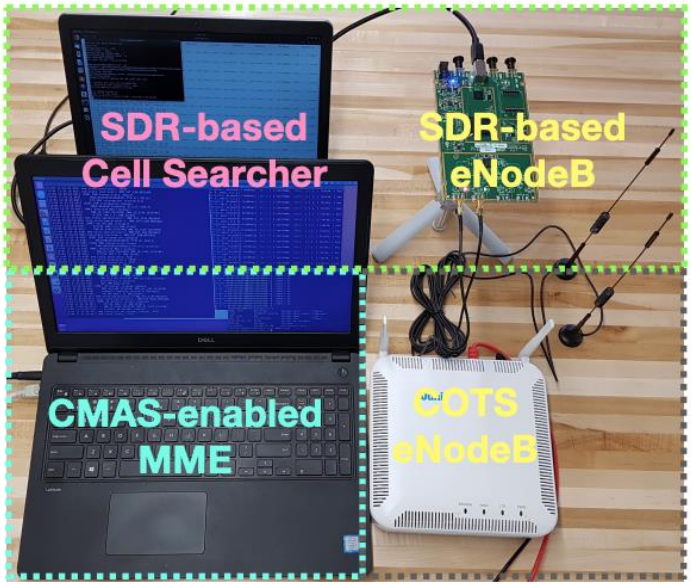


Figure 9: The Presidential Alert Spoofer scans for an eNodeB, gathers operator information, and sends a fake Presidential Alert to both idle and active UEs. The UEs may be FDD or TDD. This setup consists of one SDR device, one COTS LTE eNodeB, and 2 laptops.

University of Stavanger

Popular Security tools

Security Research tools - software

- **Network setup cost < 1500 USD**
  - Open source software & hardware

- **Network tools**
  - Osmocom Project (2G)
  - OpenBTS-UMTS (3G)
  - OpenAirInterface/openLTE /Amarisoft (4G)
  - SRSRAN (4G/5G)
  - Amarisoft/OpenAirInterface (5G)

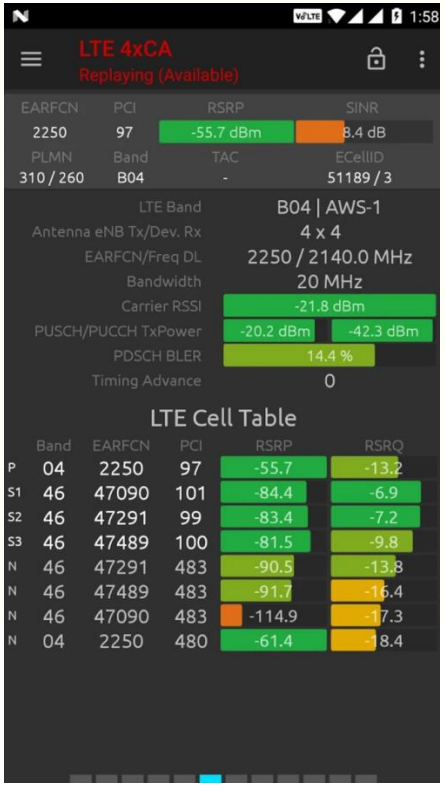
- **Mobile side tools**
  - Osmocombb (2G)
  - SRSRAN (4G/5G)

University of Stavanger

Security Research tools - hardware

- Software defined radios
  - Ettus Research
  - Myriad RF - LimeSDR

- Network monitoring software
  - Network Signal Guru (on mobile)
  - Wireshark



University of Stavanger

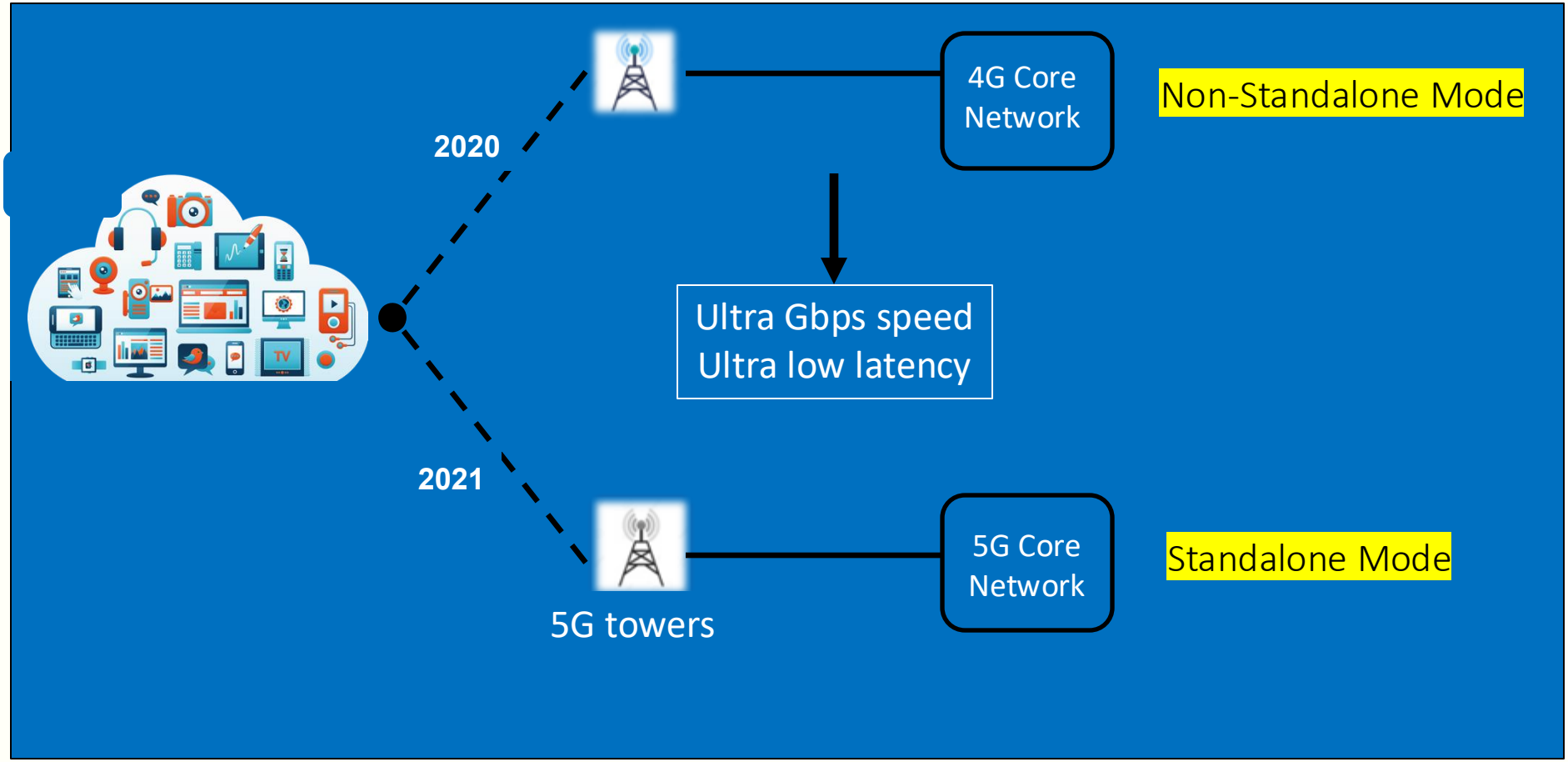
Reasons for vulnerabilities

Trade of between security and

- Performance
  - Phone restricts to connect to network- saving power
  - Saving network signaling resources (avoid unsuccessful attach)
  - Operator do not refresh temporary identifiers often
- Availability
  - Operators require unprotected reports/specific information for troubleshooting
- Functionality
  - Smartphone apps on generic platforms not mobile-network-friendly
- Attacking cost
  - Active type of IMSI catcher attacks thought to be expensive

University of Stavanger

5G Deployment Types

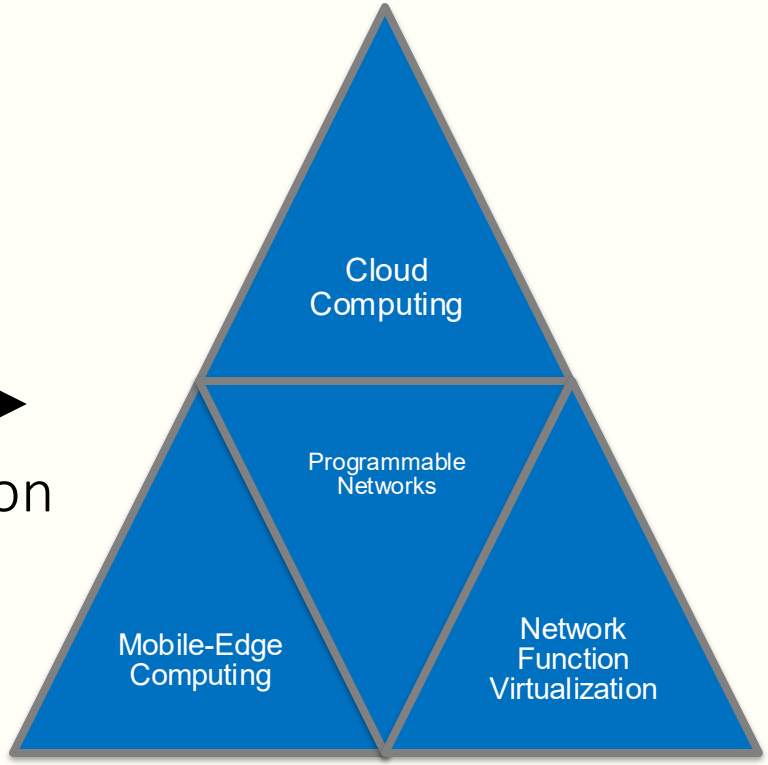


5G Architecture

5G Core Network Infrastructure

Technology

Transformation



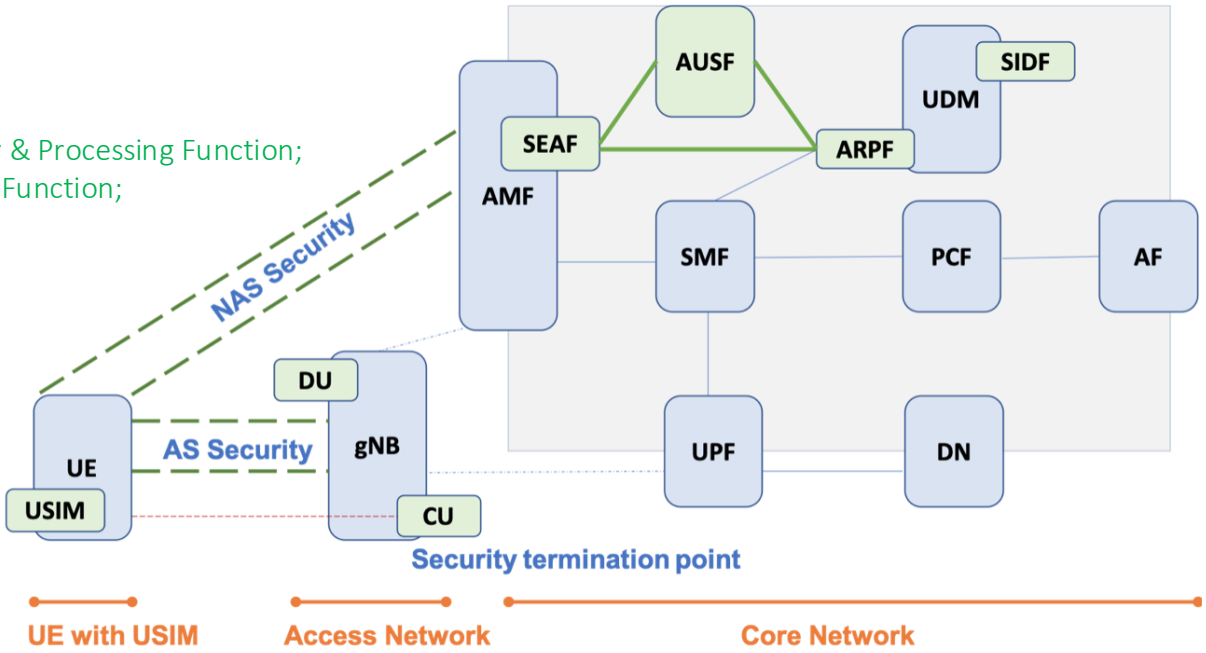
5G Architecture

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

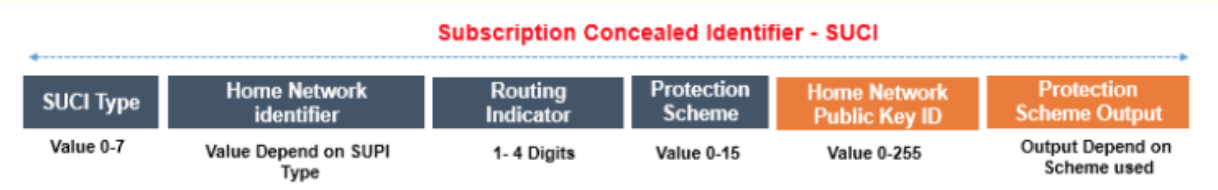
AMF - Access Management Function
SMF - Session Management Function
UDM - Unified Data Mandagement
PCF - Policy Control Function
AF- Application Function
UPF - User Plane Function
DN - Data Network

AS – Access Stratum
NAS – Non-access Stratum

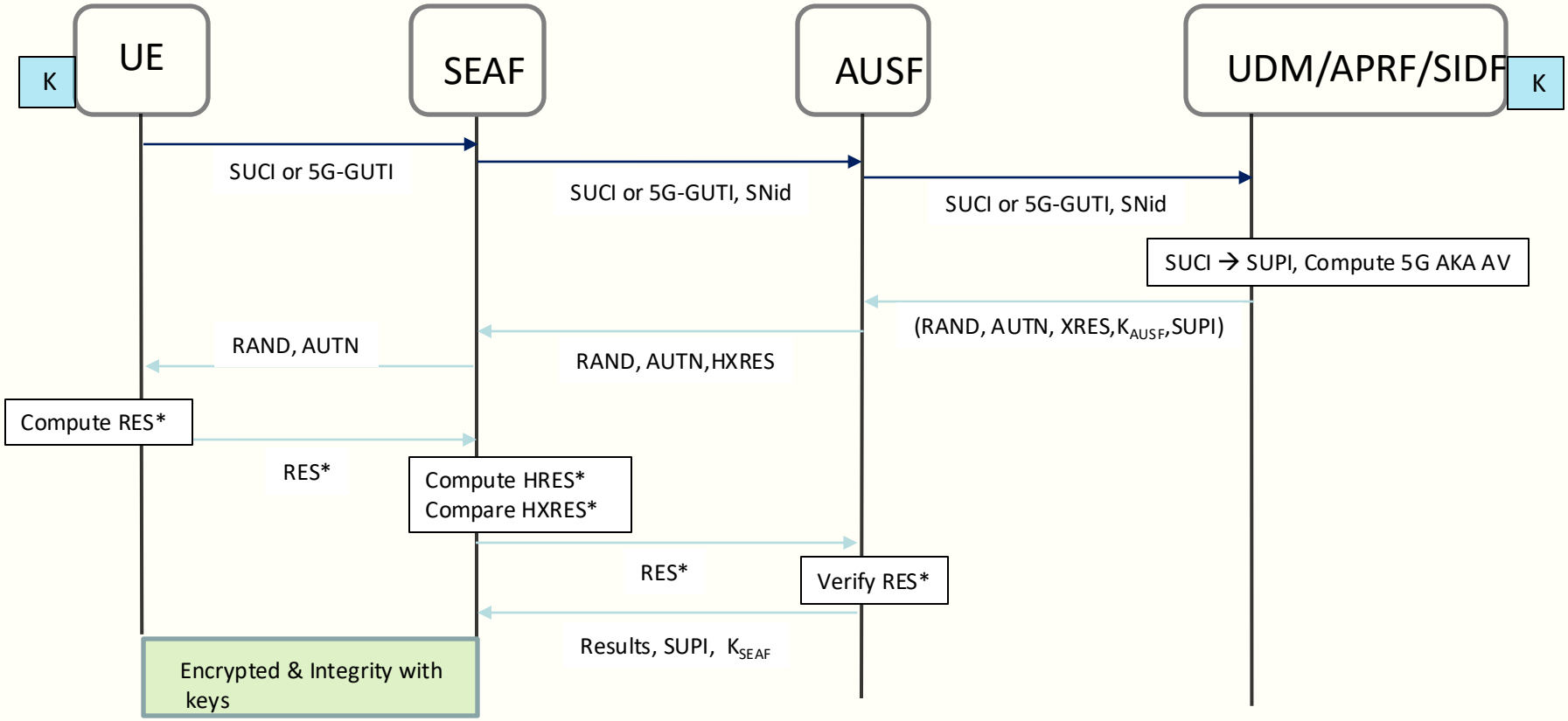


New Identifiers

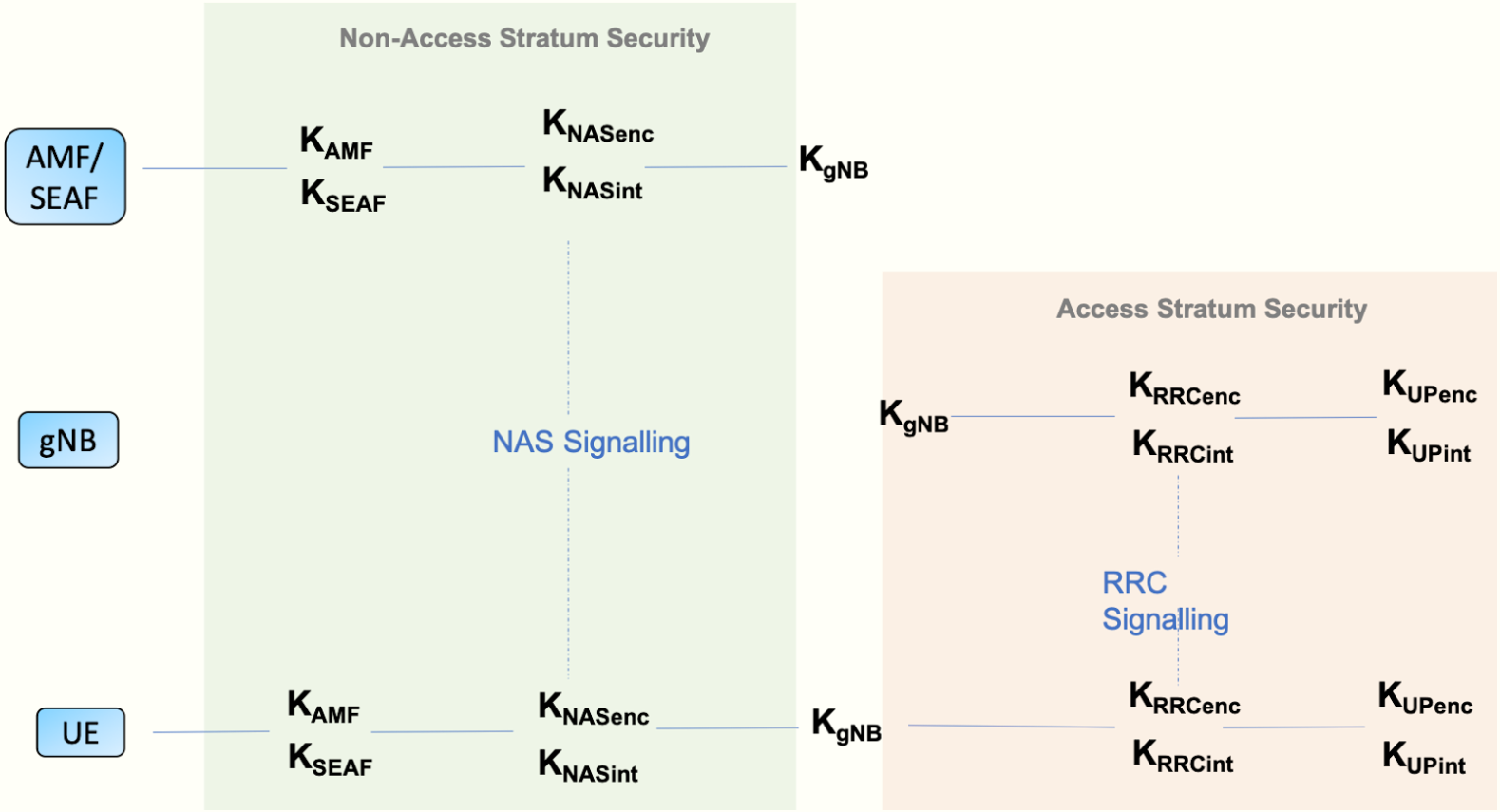
- SUCI – Subscription Concealed Identifier
- SUPI – Subscription Permanent Identifier
- Public key of the home network operator



5G Authentication Protocol - AKA

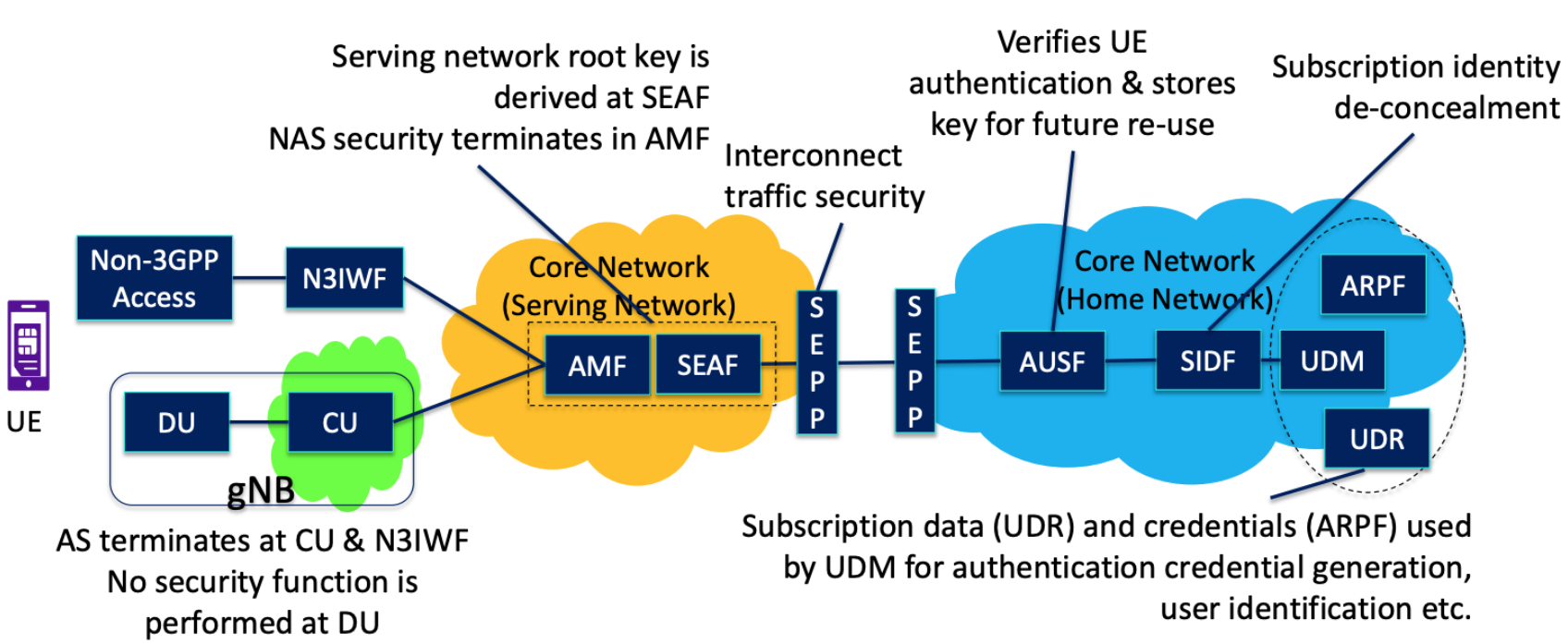


5G Authentication Protocol – Key Hierarchy



University of Stavanger

Security Functions in 5G Architecture



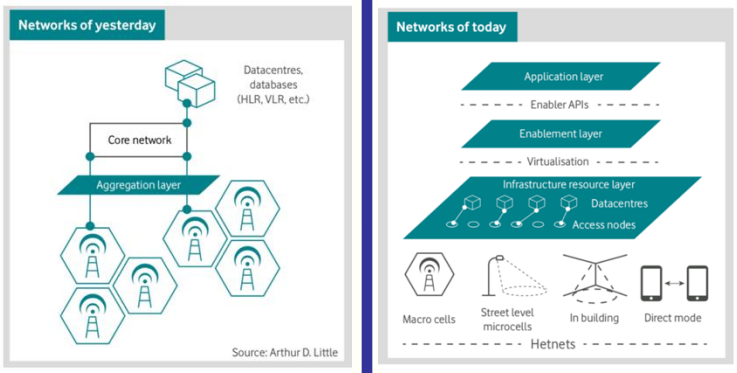
Source: Anand Prasad, RSA 2019

University of Stavanger

5G Security Issues

Comparison with previous generations

- Separated CN & RAN
- Dedicated IT hardware/software
- Propriety signalling protocols (Diameter/SS7)
- Difficult to modify for new services

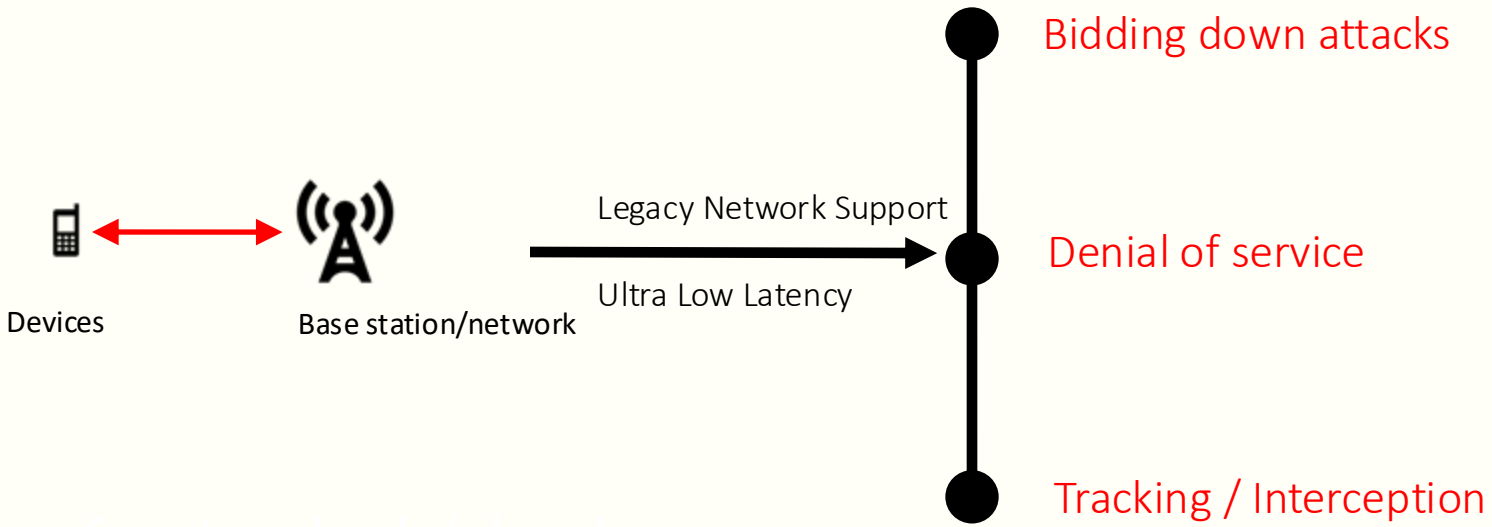


- Less separated CN & RAN
- Configurable Software/hardware
- Web based signalling protocols (HTTP, TLS, REST)
- APIs for creating new services

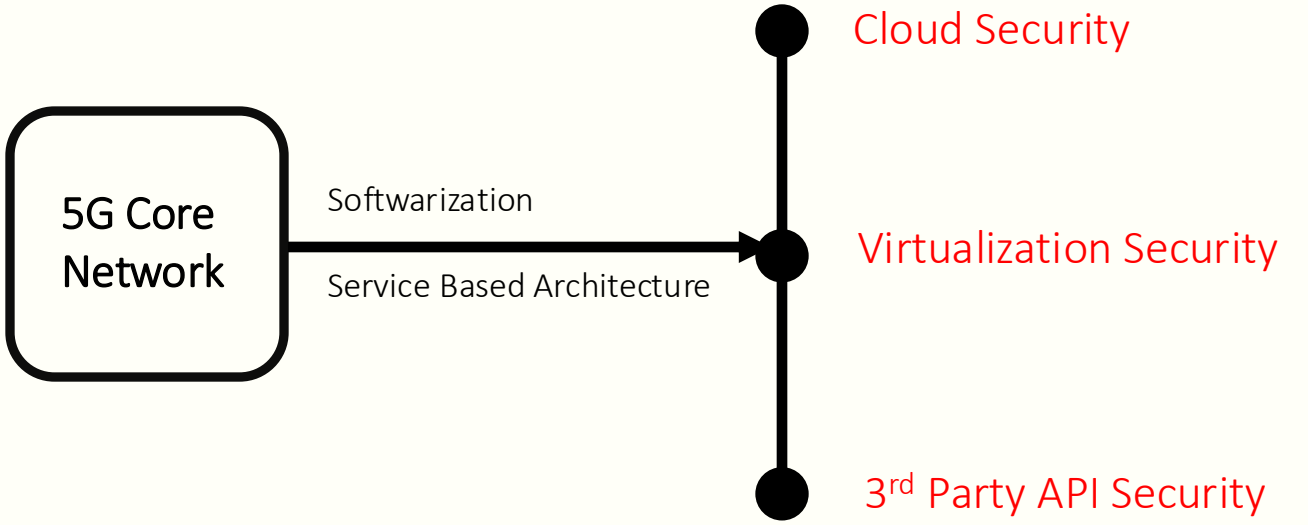
figure- Vodafone Whitepaper

University of Stavanger

Increased Attack Surface



Increased Attack Surface



Security challenges..

Denial of Service / Distributed Denial of Service attack protection

Botnet?

21 billion by 2020

Bandwidth per device

5 Gbps

Average wired broadband speed

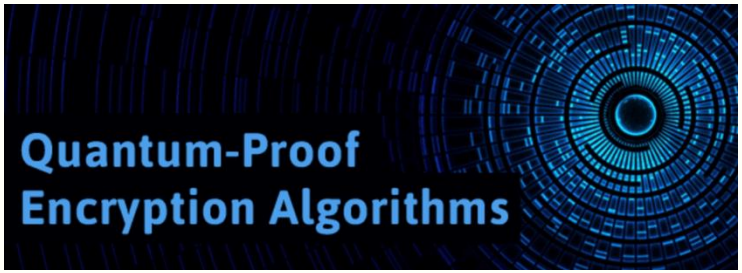
Rank	Country	Average Download Speed (Mbps)	Total Tests	Time To Download HD Movie (5GB)
1	Singapore	**60.39**	524,018	11 Mins, 18 Secs
2	Sweden	**46.00**	367,241	14 Mins, 50 Secs
3	Denmark	**43.99**	150,529	15 Mins, 31 Secs
4	Norway	**40.12**	86,920	17 Mins, 01 Secs
5	Romania	**38.60**	175,948	17 Mins, 41 Secs

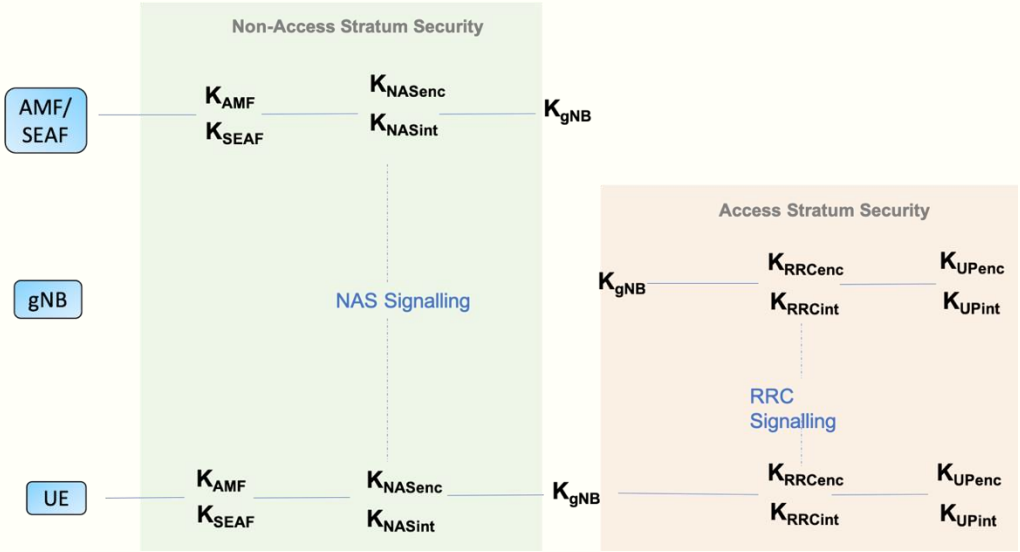
Source: Fastmetrics

University of Stavanger

Security challenges..

Cellular encryption algorithms and techniques





Meanwhile in Norway -

Country			Spain			France	United States				Beijing			Norway				
Operator			A	B		A	A		B	C	A	B	C	1	2	3	3	4
Deployment type: SA vs. NSA			NSA	NSA		NSA	SA	NSA	NSA	NSA	SA	SA	SA	NSA	NSA	NSA	SA	Priv. SA
Subscriber Identifiers	Ciphering of Permanent Identifiers																	
	GUTI Refresh	After Registration																
		Periodic Registration									—	—	—					
		After Service Request (Paging)																—
Authentication Procedure	5G AKA										—	—	—					
Control Plane Data (CP)	Confidentiality	NAS	EEA2	EEA2/1	EEA2/1	EEA2	NEA2	EEA2	EEA2	EEA3				EEA1	EEA2	EEA2	5G-EA0	5G-EA1
		RRC	EEA2	EEA2/1	EEA2/1	EEA2	NEA2	EEA1	EEA2	EEA2				EEA2	EEA2	EEA2	NEA2	NEA0
	Integrity	NAS	EIA2	EIA2	EIA2	EIA2	NIA2	EIA2	EIA2	EIA3				EIA1	EIA2	EIA2	5G-IA2	5G-IA1
		RRC	EIA2	EIA2	EIA2	EIA2	NIA2	EIA2	EIA2	EIA2				EIA2	EIA2	EIA2	NIA2	NIA2
User Plane Data (UP)	Confidentiality		NEA2	NEA2	NEA2	NEA2	NEA2	NEA2	NEA2	NEA2								
	Integrity						NIA2		NIA2									
Initial NAS message	Protection																	
UE Radio Capabilities Transmission after RRC SMC											—	—	—	—	—	—	—	—

5G Compliant | 4G Compliant | No security | Not observed

Figure F.1: Extension of Related Works Table Full Size

Thank You.

Questions?

References

1. 3GPP System Architecture Evolution (SAE); Security architecture - https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296
2. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices - https://ieeexplore.ieee.org/document/5958024
3. Breaking LTE on Layer Two - https://alter-attack.net/
4. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols - https://content.sciendo.com/view/journals/popets/2019/3/article-p108.xml?language=en
5. New privacy issues in mobile telephony: fix and verification - https://dl.acm.org/doi/10.1145/2382196.2382221
6. This is Your President Speaking: Spoofing Alerts in 4G LTE Networks- https://dl.acm.org/doi/10.1145/3307334.3326082
7. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities - https://dl.acm.org/doi/10.1145/3317549.3319728
8. Practical attacks against privacy and availability in 4g/lte mobile communication systems - https://www.ndss-symposium.org/wp-content/uploads/2017/09/practical-attacks-against-privacy-availability-4g-lte-mobile-communication-systems.pdf
9. Security architecture and procedures for 5G System - https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169
10. 4G to 5G Evolution: In-Depth Security Perspective - https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/12989/IDY-F01-4G-to-5G-Evolution-In-Depth-Security-Perspective.pdf

University of Stavanger