

Wireless Security (4G/5G Cellular Networks)

Dr. Ravishankar Borgaonkar

DAT-510

22 October 2024

Outline

- Wireless Security & 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?

Wireless vs Wired Security

- **Channel**

- Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks
- Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols

- **Mobility**

- Wireless devices are far more portable and mobile than wired devices
- This mobility results in a number of risks

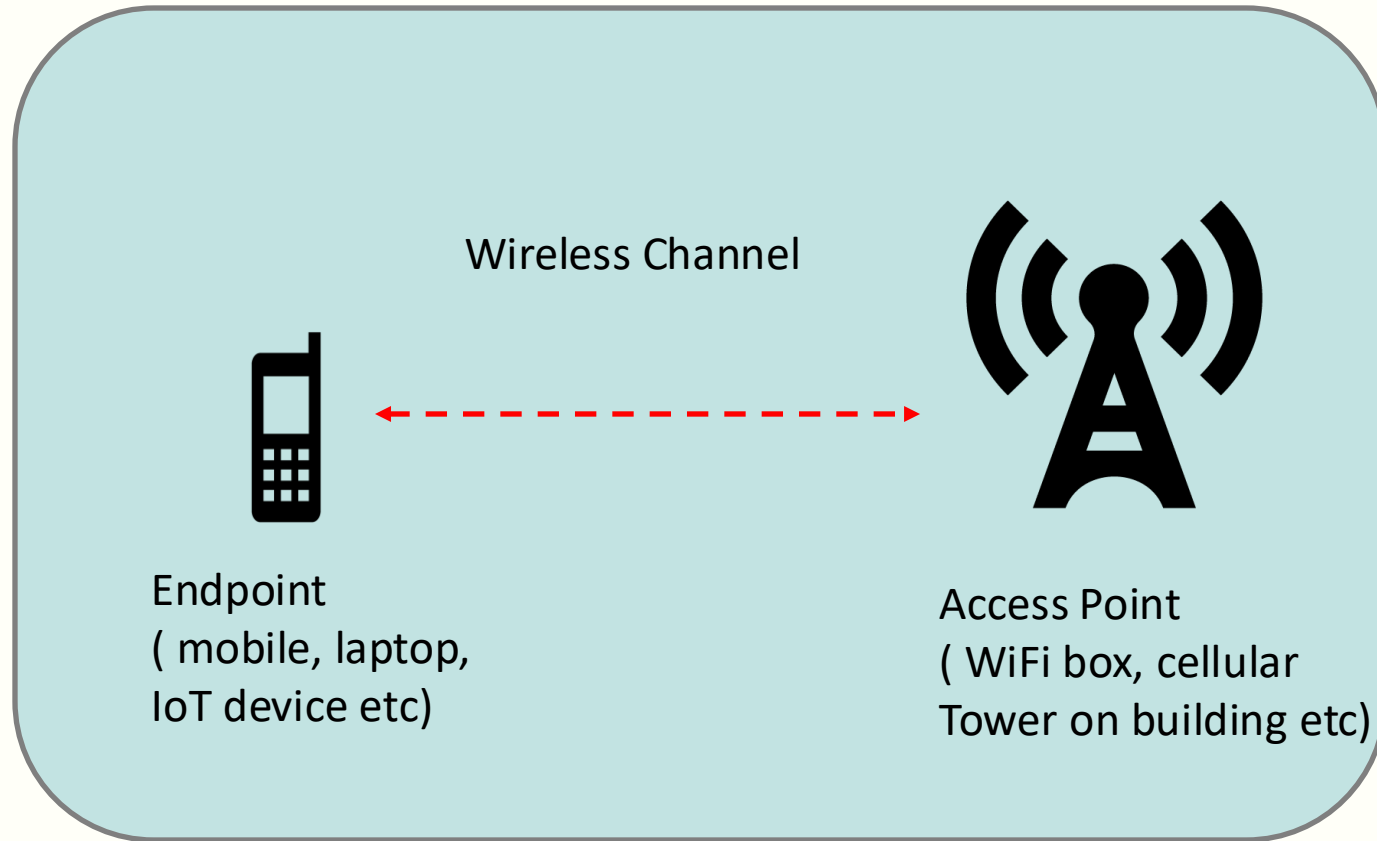
- **Resources**

- Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware

- **Accessibility**

- Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations

Wireless Network Components



1G Networks – wireless era

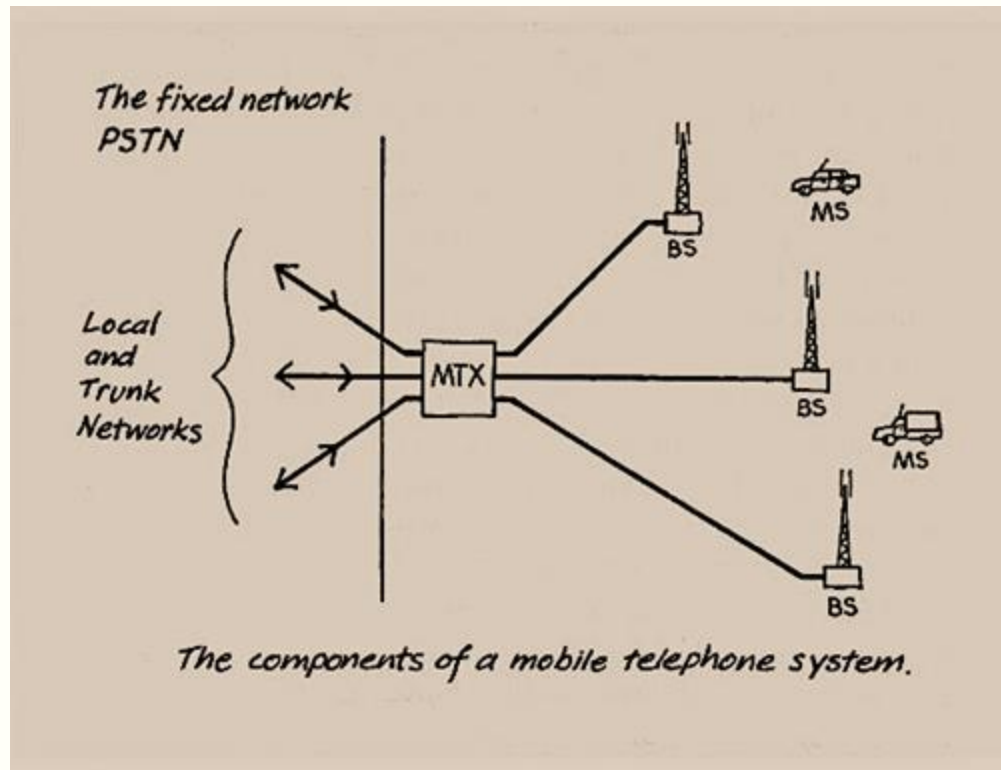


figure- Ericsson History

Problems with 1G

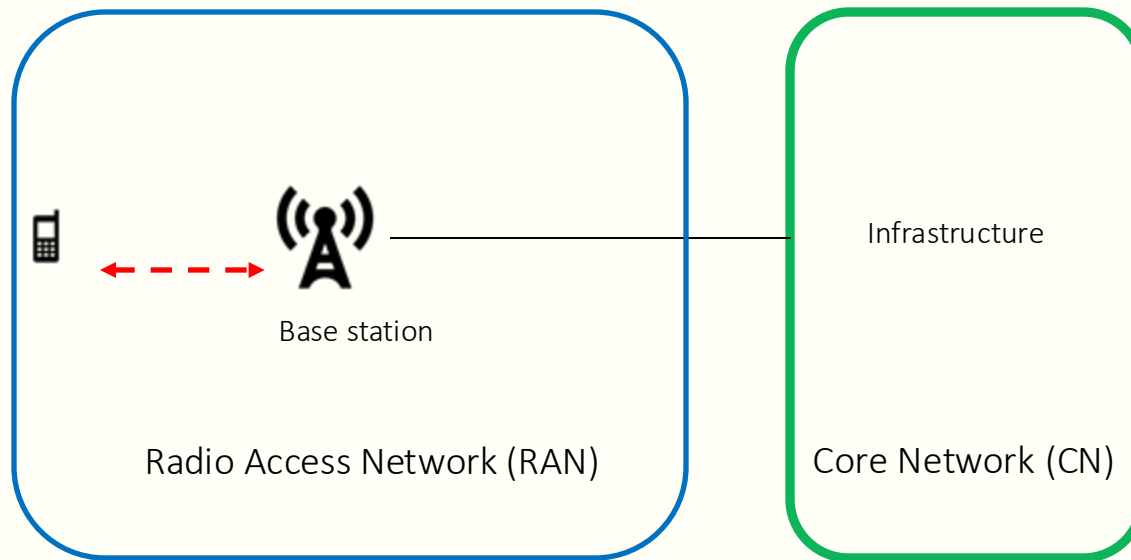
- No authentication & encryption
- Heavy devices
- No roaming – international calls
- But still luxury of talking to loved ones

Stakeholders & Roles

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



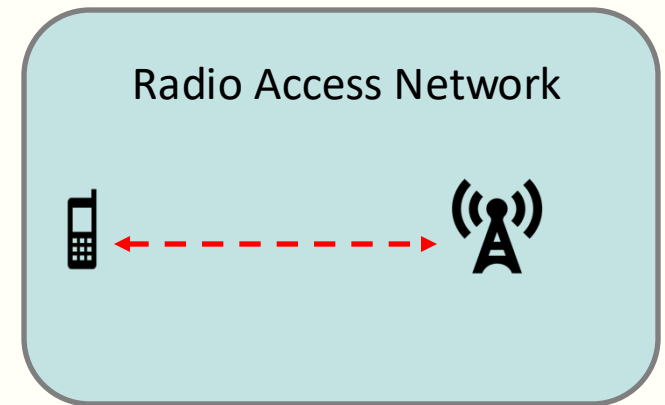
General Cellular Network Architecture



Note: picture provides an abstract view only

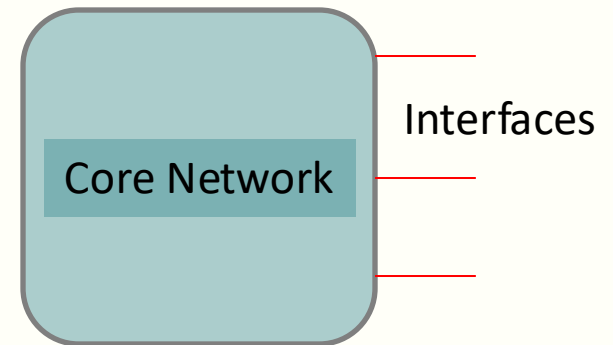
Threats to RAN

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



Threats to Core Network

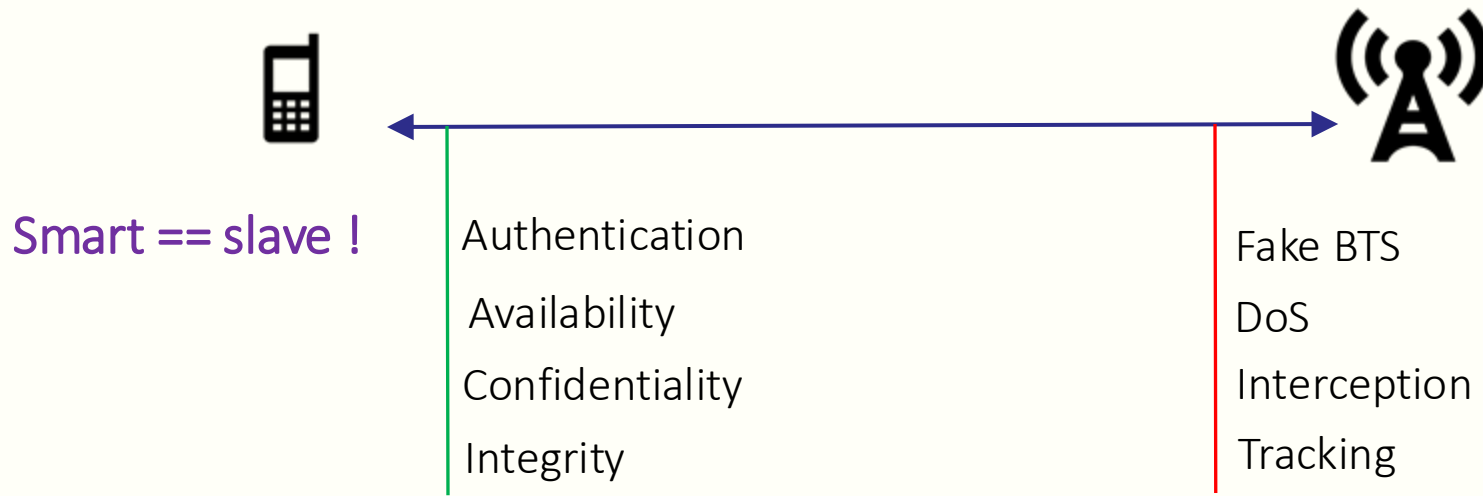
- Espionage
- Insider attacks
- Location tracking
- Billing frauds
- Denial of service



Security aspects



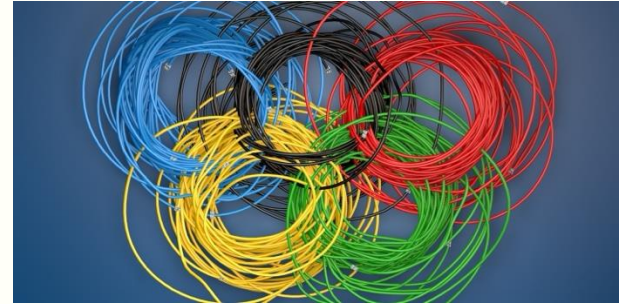
Security aspects & threats



Security tradeoffs play essential role in protocol design!

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.

Security Principles

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

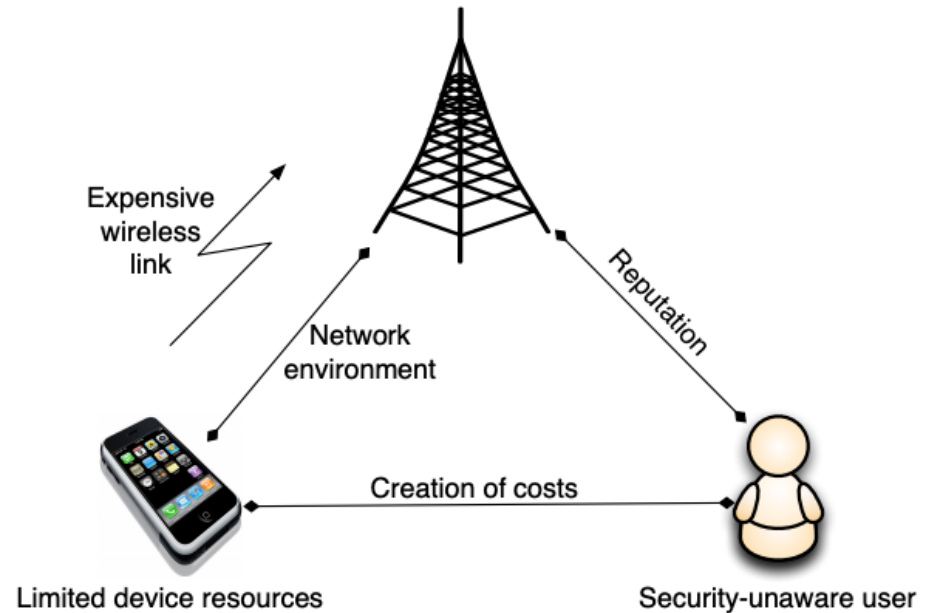


Figure 1. Specifics of Mobile Devices

Authentication in 4G/5G 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



SIM Data – related to authentication

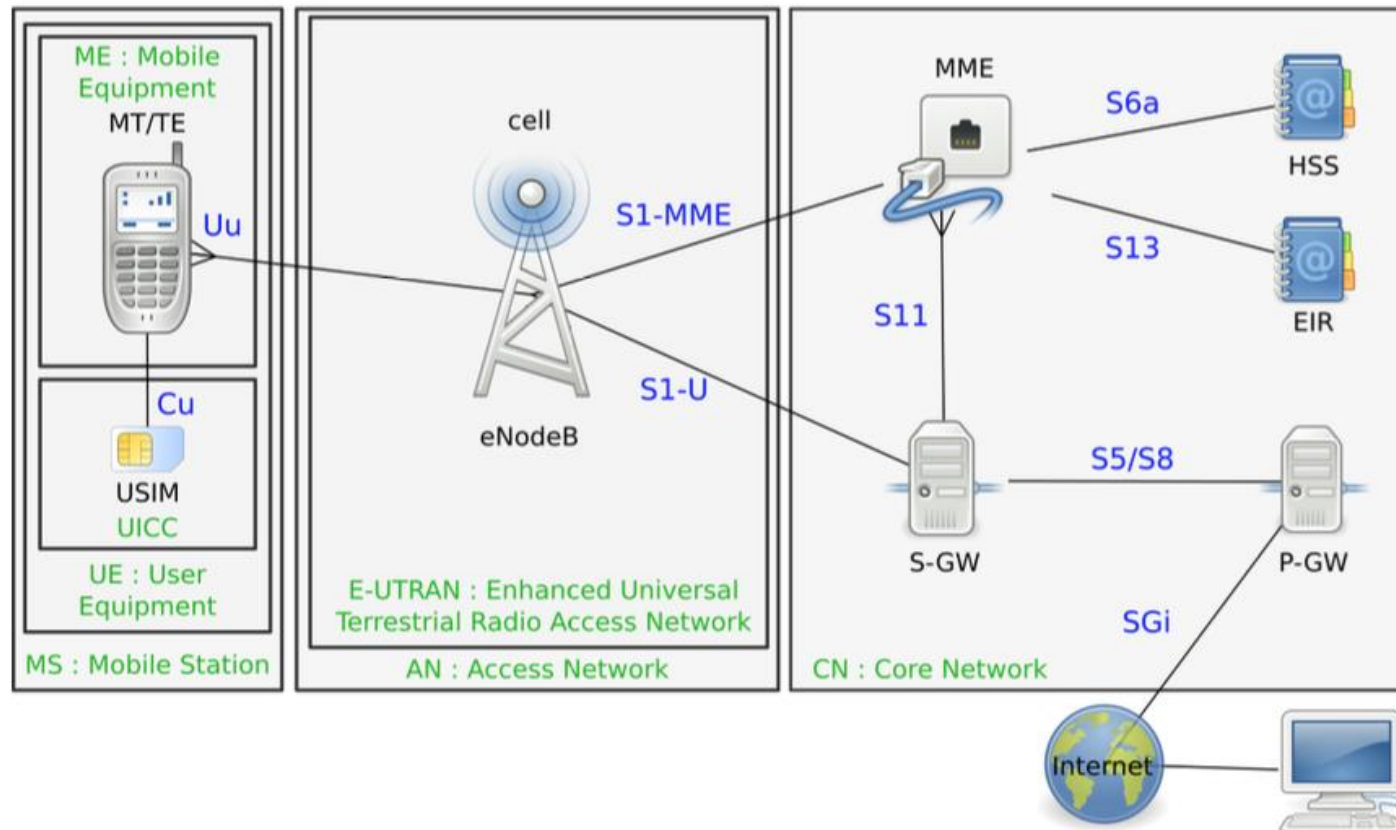
- Integrated Circuit Card ID (ICC-ID) (aka SIM Serial Number - SSN)
 - Uniquely identifies a SIM card (hardware)
- International Mobile Subscriber Identity Module (IMSI)
 - Uniquely identifies the mobile subscriber (15 digits, ITU E.212 standard)
 - MCC (3 digits), MNC (2 or 3 digits), MSIN (9 or 10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

Security in SIM cards

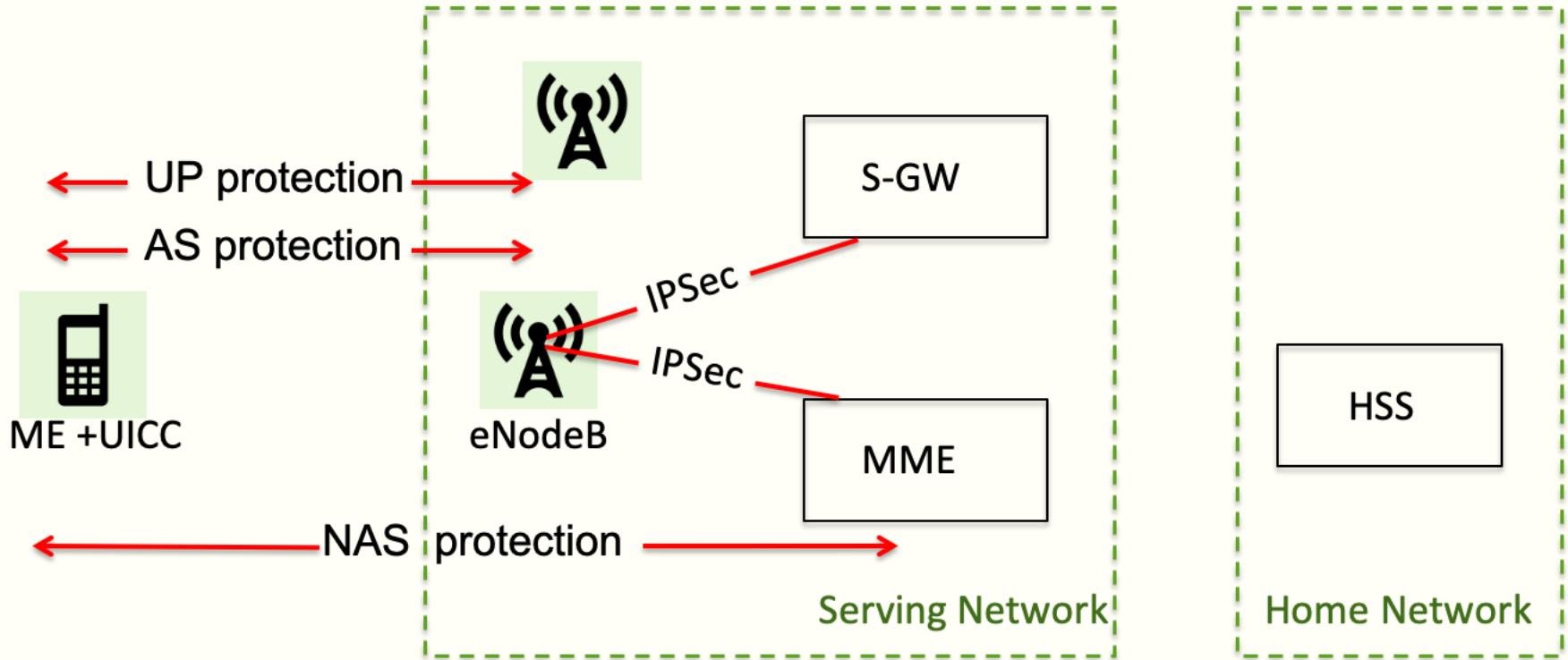
- Identity and Access control (IMSI, PIN1/PIN2, PUK code)
- Authentication to network operator (Ki, A3)
- Confidentiality (Kc, A8)
- Anonymity (TMSI)
- SIM application toolkit

4G/LTE Network Architecture

Structure of an LTE network



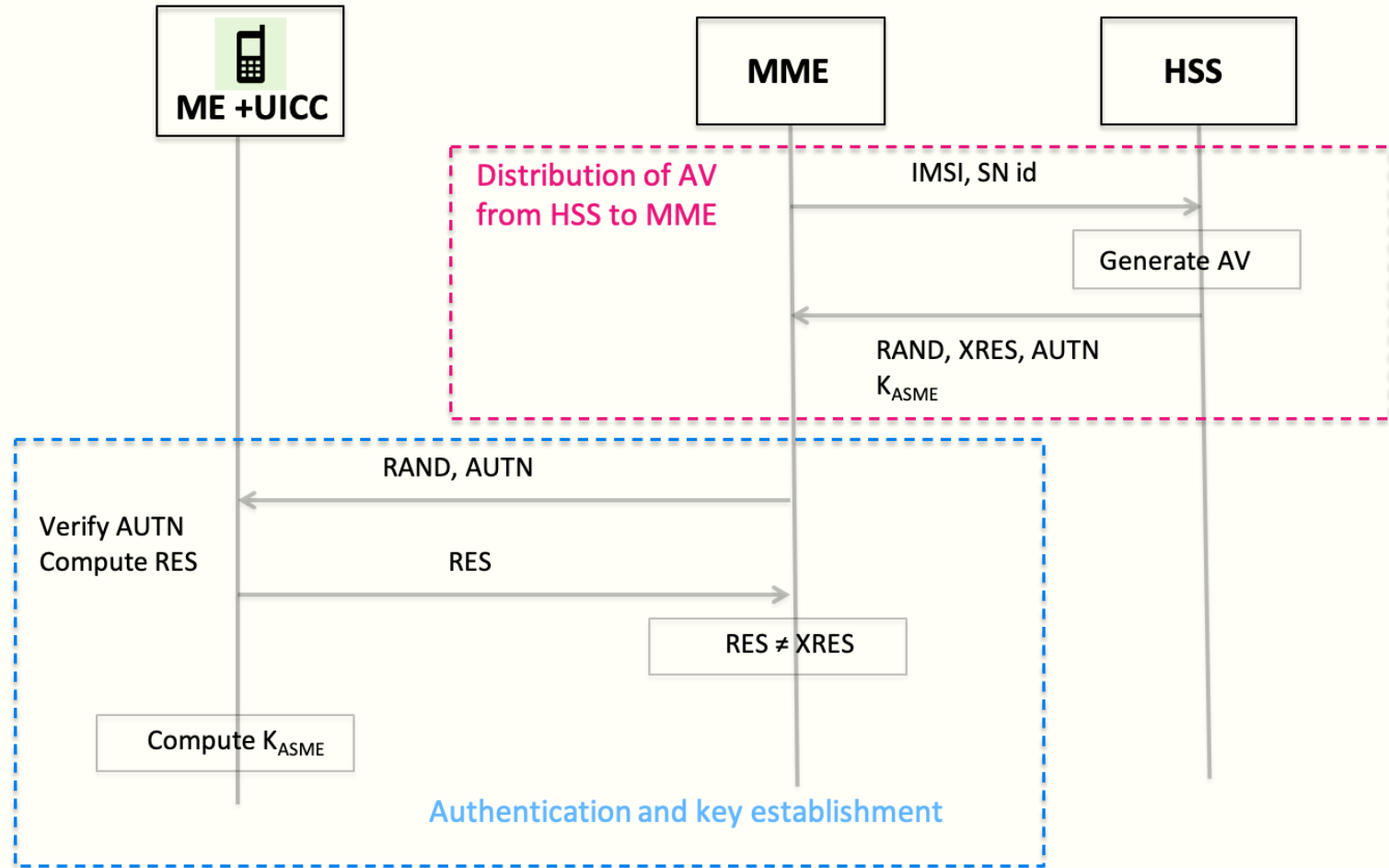
4G security architecture



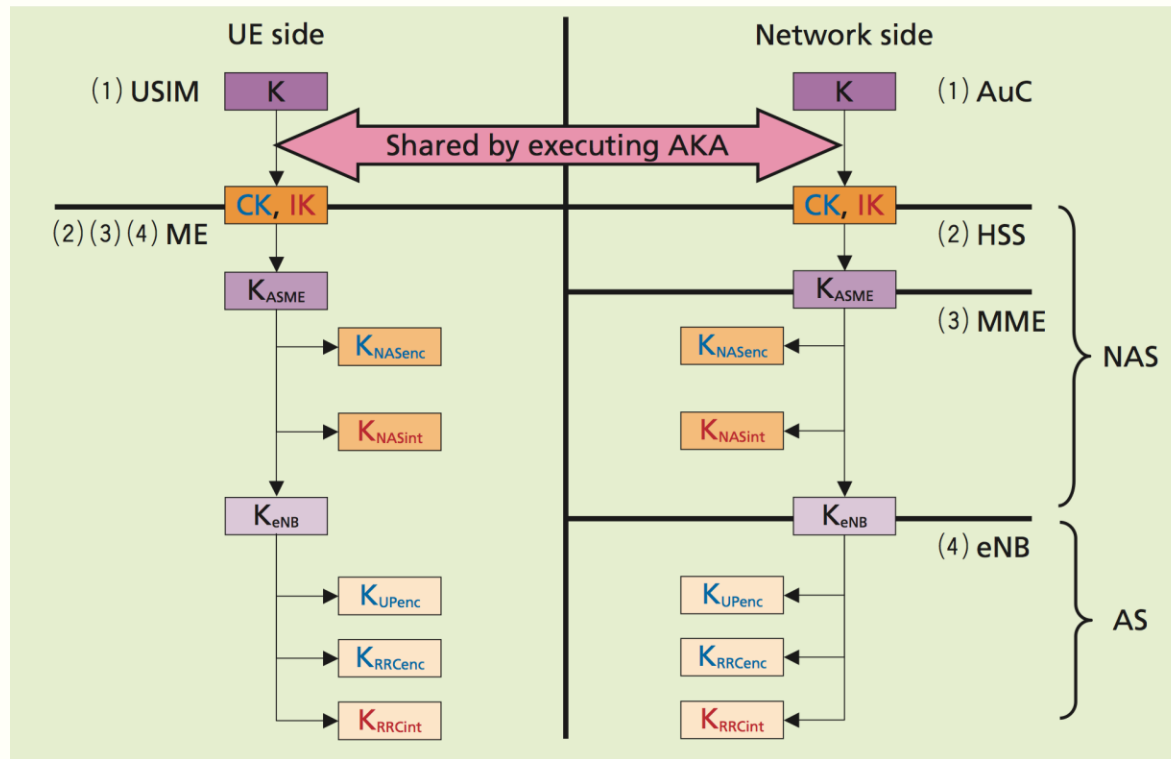
ME Mobile Equipment
UICC Universal Integrated Circuit Card
eNodeB Evolved NodeB
AS Access Stratum
UP User Plane

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

4G AKA protocol (simplified)



Key hierarchy



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

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

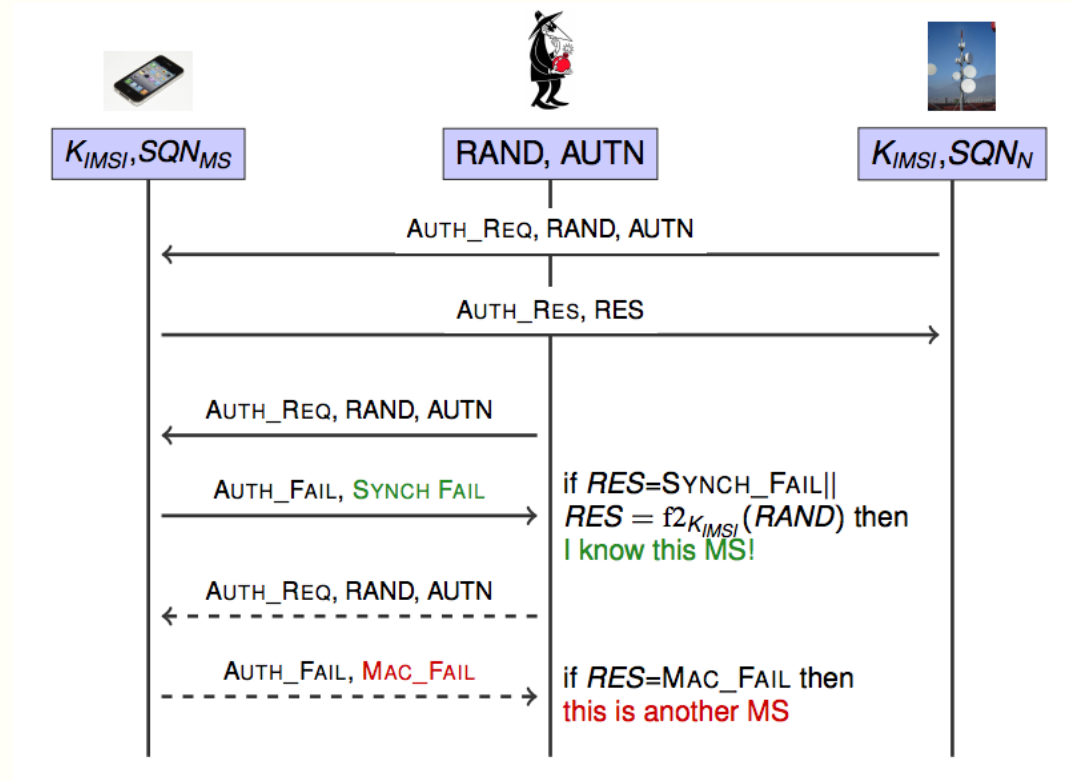
**Small cellular base-sta
homeland security app**



**3G-GSM TACTICAL
INTERCEPTION &
TARGET LOCATION**

3G/4G AKA vulnerability

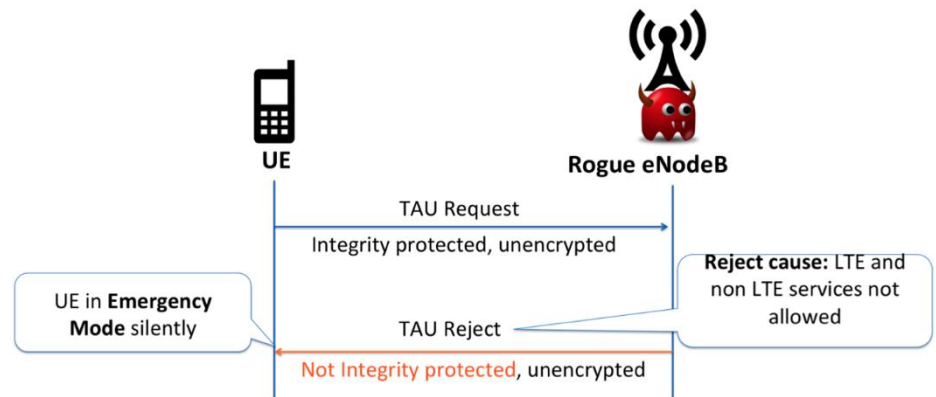
- Linkability attack by Arpanis et al
- Affects in 4G as well
- IMSI catcher type attacks



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



SMS spoofing Attacks

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



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.

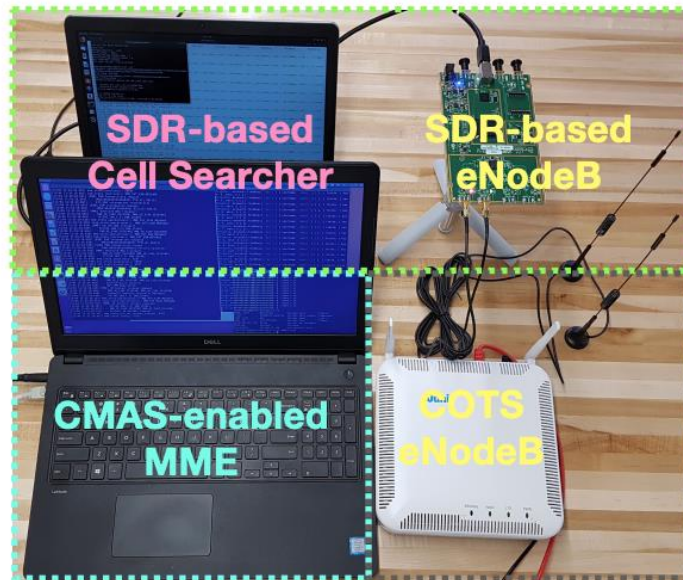
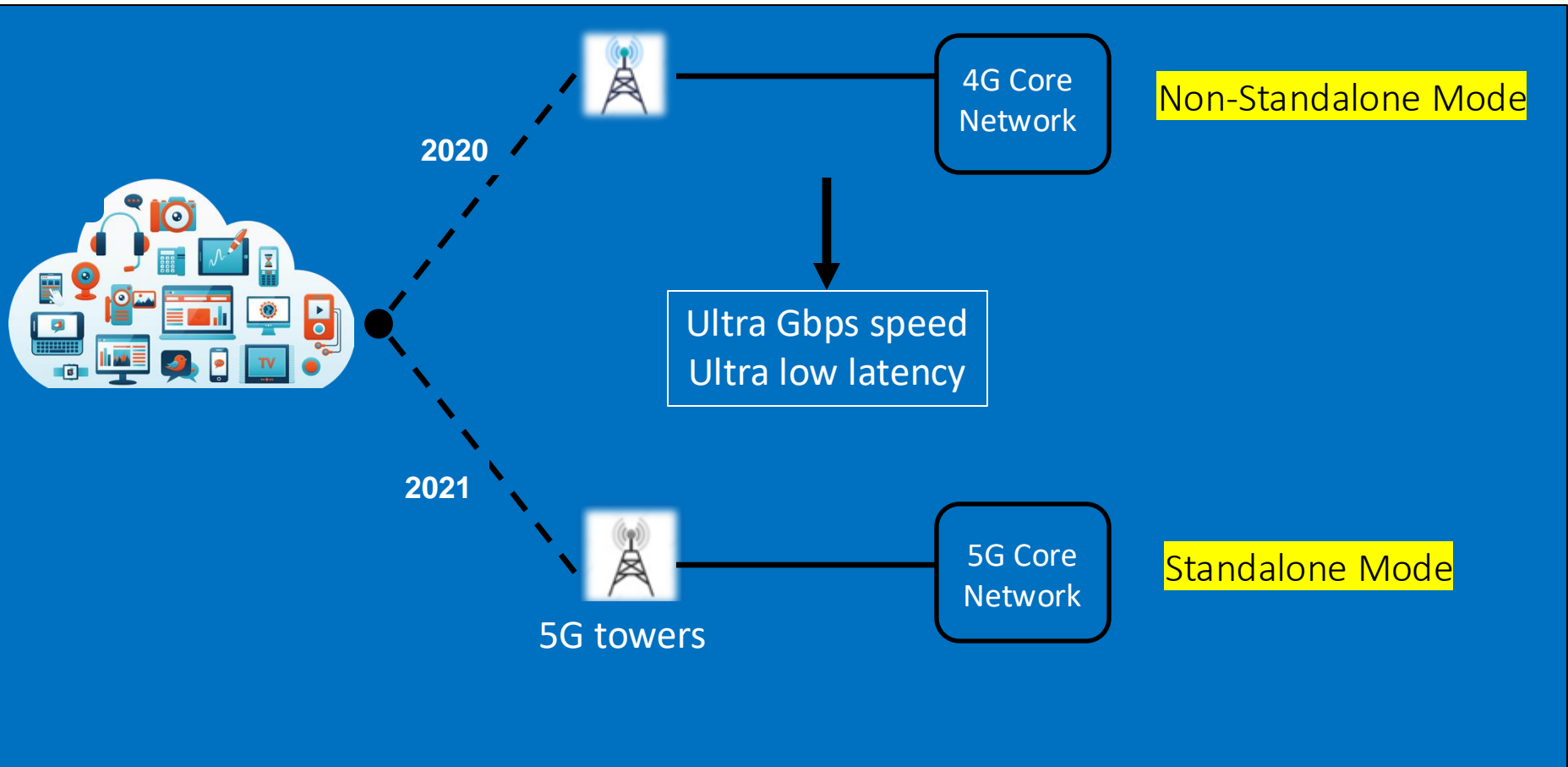
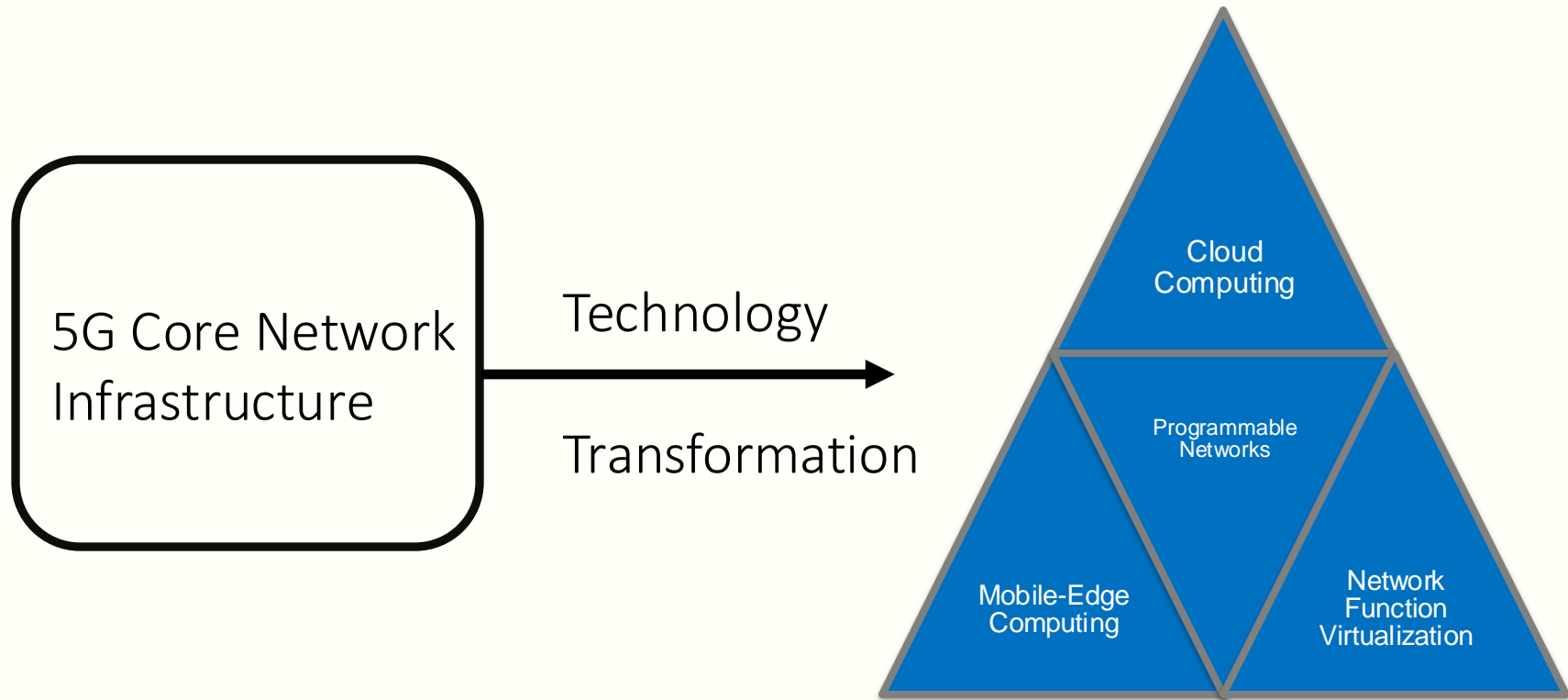


Figure 9: The Presidential Alert Spoofer scans for an eNodeB, gathers operator information, and sends a fake Presidential Alert to both idle and active UEs. The UEs may be FDD or TDD. This setup consists of one SDR device, one COTS LTE eNodeB, and 2 laptops.

5G Deployment Types



5G Architecture



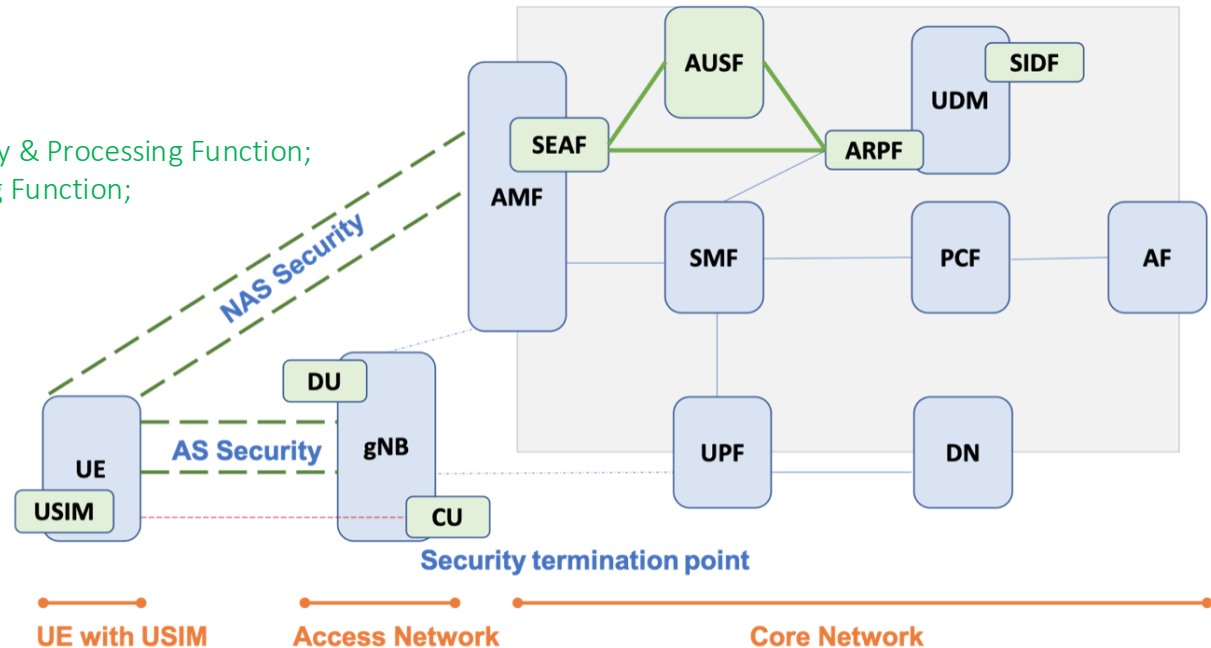
5G Architecture

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 - Scurity 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

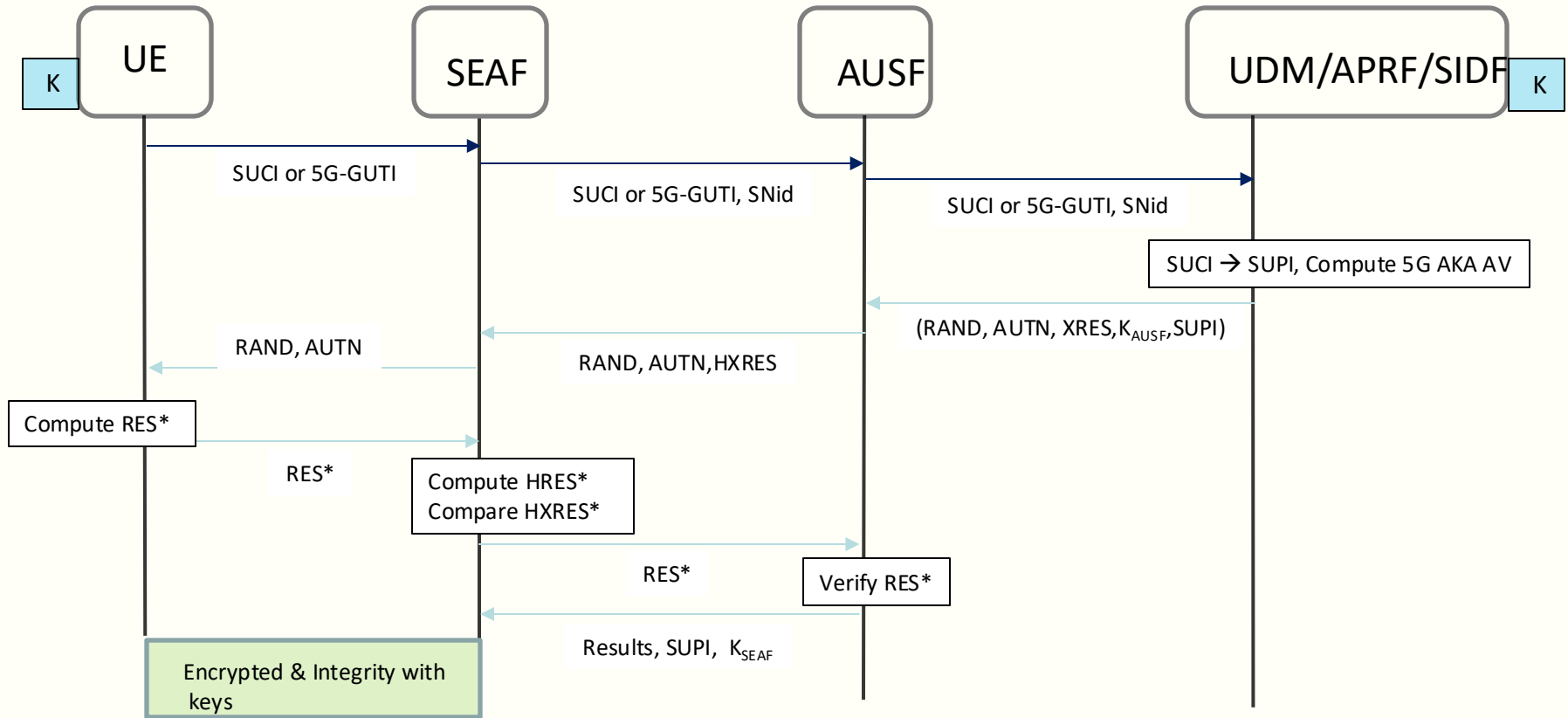


New Identifiers

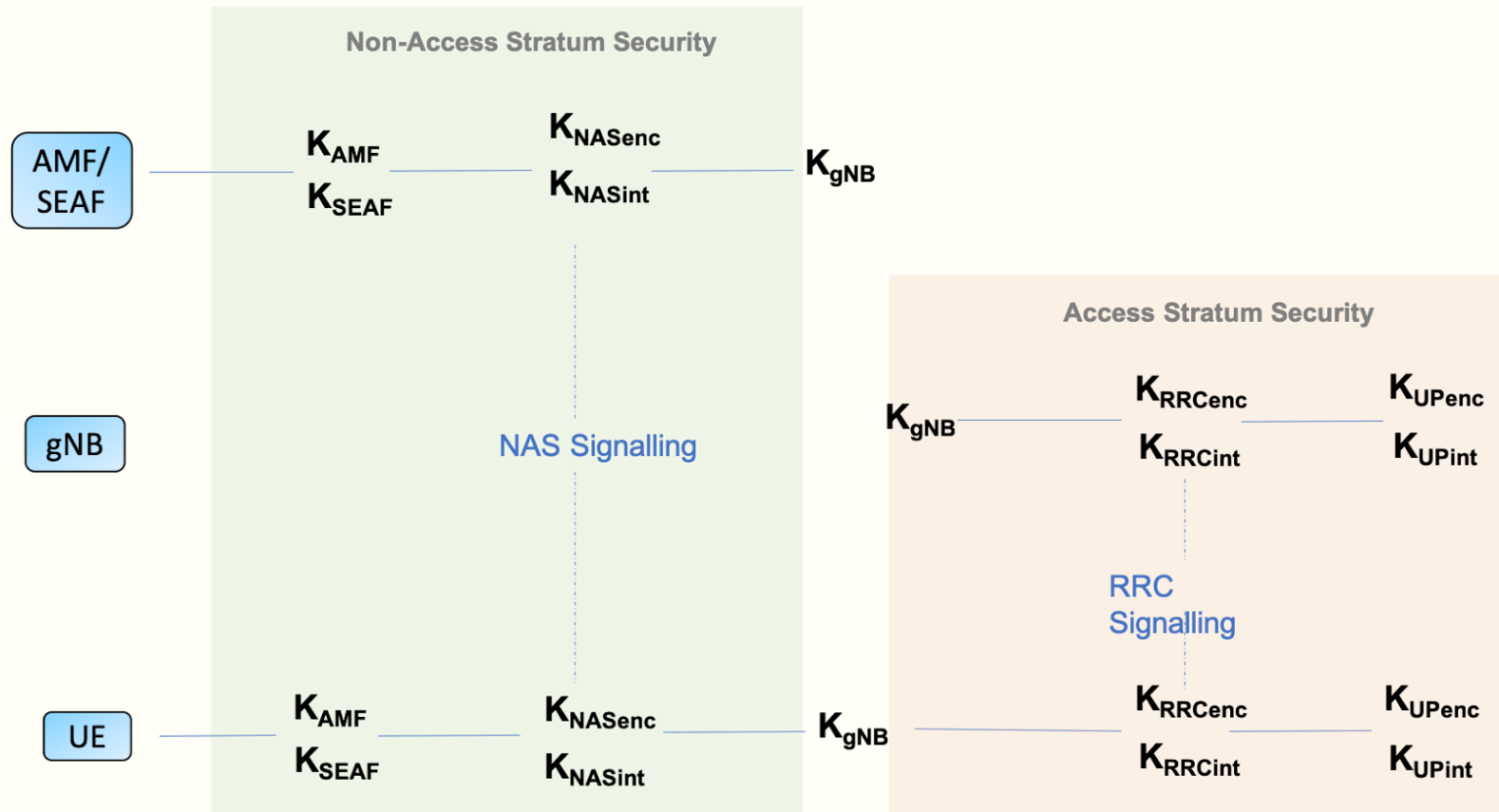
- SUCI – Subscription Concealed Identifier
- SUPI – Subscription Permanent Identifier
- Public key of the home network operator



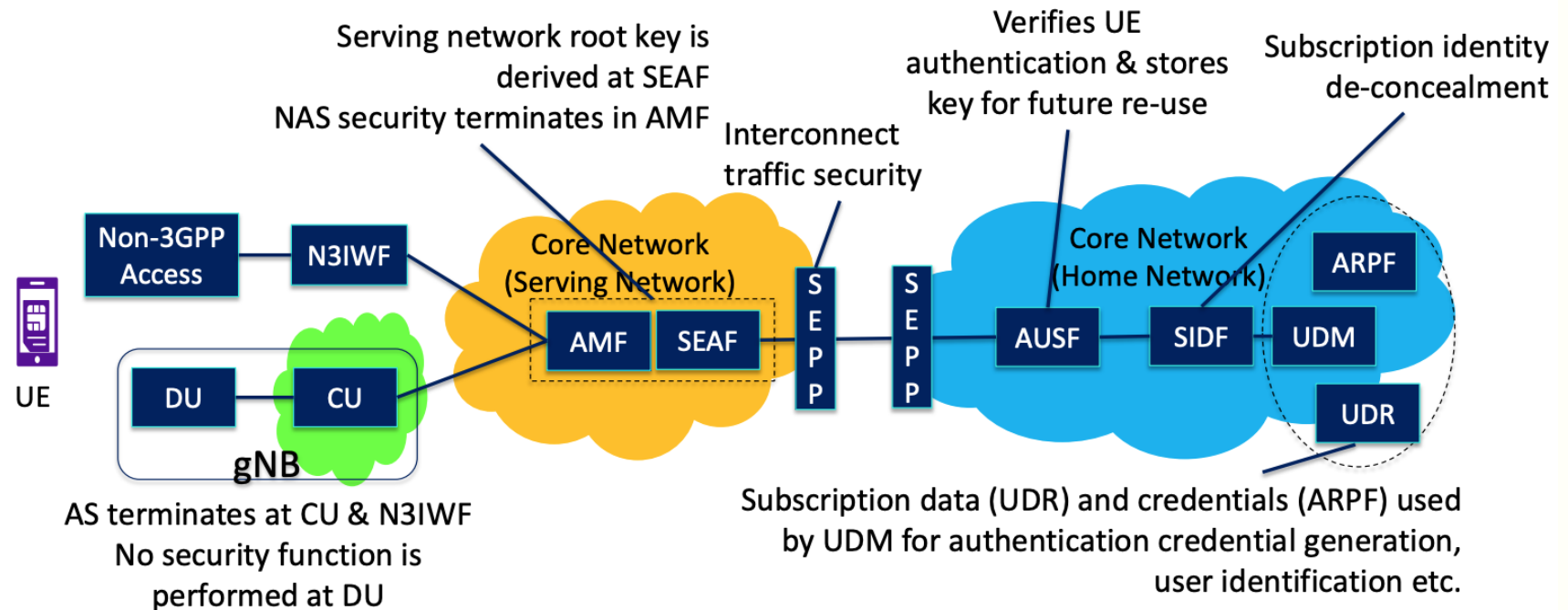
5G Authentication Protocol - AKA



5G Authentication Protocol – Key Hierarchy



Security Functions in 5G Architecture

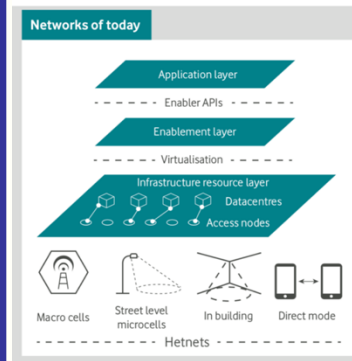
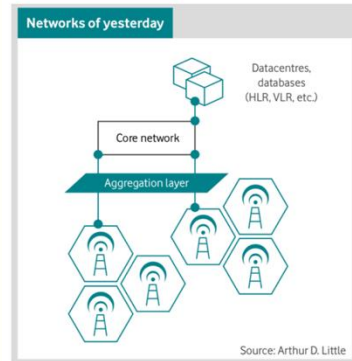


Source: Anand Prasad, RSA 2019

5G Security Issues

Comparison with previous generations

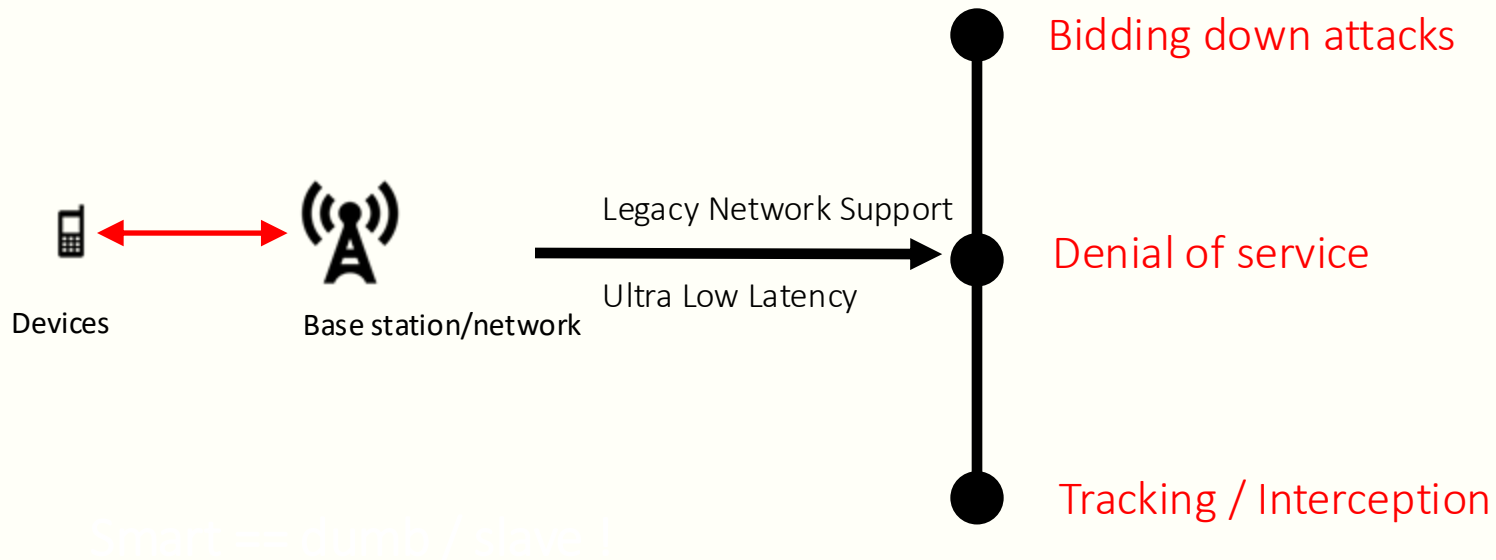
- Separated CN & RAN
- Dedicated IT hardware/software
- Proprietary signalling protocols (Diameter/SS7)
- Difficult to modify for new services



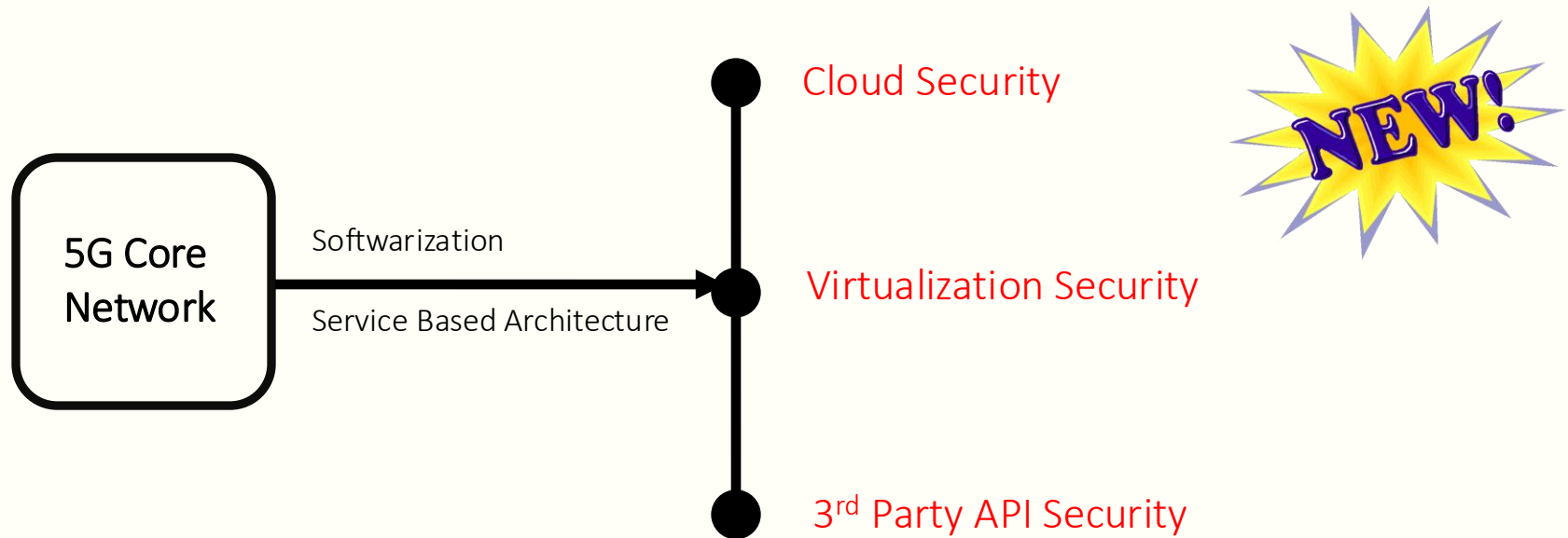
- Less separated CN & RAN
- Configurable Software/hardware
- Web based signalling protocols (HTTP, TLS, REST)
- APIs for creating new services

figure- Vodafone Whitepaper

Increased Attack Surface



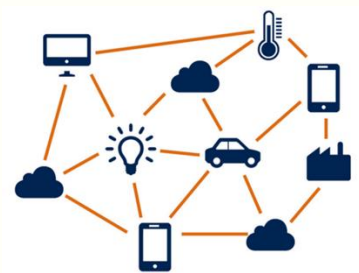
Increased Attack Surface



Security challenges..

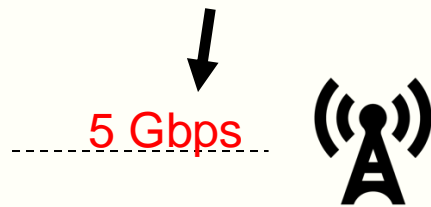
Denial of Service / Distributed Denial of Service attack protection

Botnet?



21 billion by 2020

Bandwidth per device



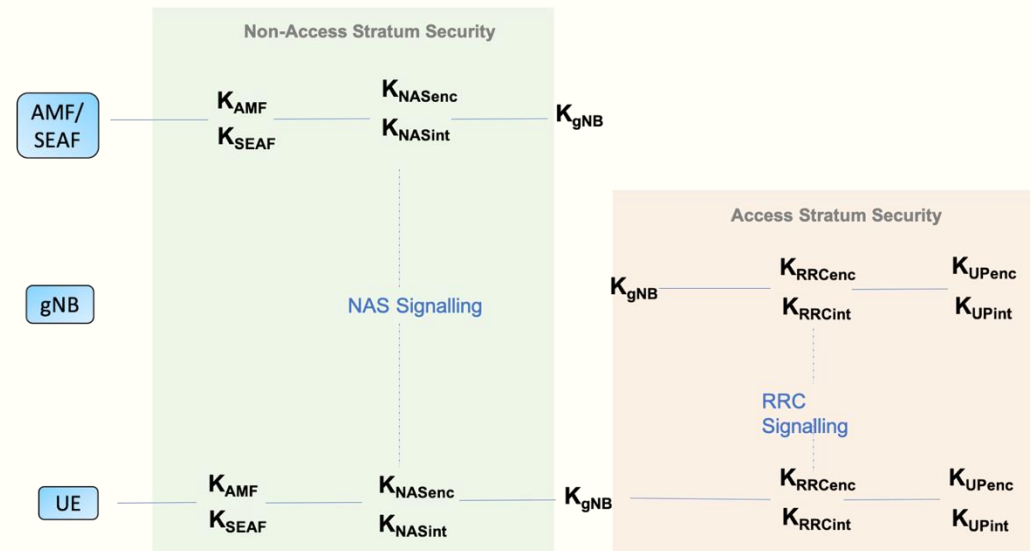
Average wired broadband speed

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

Security challenges..

Cellular encryption algorithms and techniques



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>

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)



Security Research tools - hardware

- Software Defined Radios
 - Ettus Research
 - Myriad RF - LimeSDR
- Network monitoring software
 - Network Signal Guru (on mobile)
 - Wireshark



The screenshot shows the "LTE 4xCA" application interface. At the top, it says "Replaying (Available)". Below this, there are several rows of data including EARFCN, PCI, RSRP, SINR, PLMN, Band, TAC, and ECellID. A section titled "LTE Band" shows "B04 | AWS-1" with details like "Antenna eNB Tx/Dev. Rx: 4 x 4", "EARFCN/Freq DL: 2250 / 2140.0 MHz", "Bandwidth: 20 MHz", "Carrier RSSI: -21.8 dBm", "PUSCH/PUCCH TxPower: -20.2 dBm, -42.3 dBm", "PDSCH BLER: 14.4 %", and "Timing Advance: 0". At the bottom, there is an "LTE Cell Table" with columns for Band, EARFCN, PCI, RSRP, and RSRQ, listing various cellular signals.

	Band	EARFCN	PCI	RSRP	RSRQ
P	04	2250	97	-55.7	-13.2
S1	46	47090	101	-84.4	-6.9
S2	46	47291	99	-83.4	-7.2
S3	46	47489	100	-81.5	-9.8
N	46	47291	483	-90.5	-13.8
N	46	47489	483	-91.7	-16.4
N	46	47090	483	-114.9	-17.3
N	04	2250	480	-61.4	-18.4

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