KAITIAKI

4G to 5G : New Attacks

Altaf Shaik
(Technische Universität Berlin, Germany)

Ravishankar Borgaonkar
(SINTEF Digital, Norway)

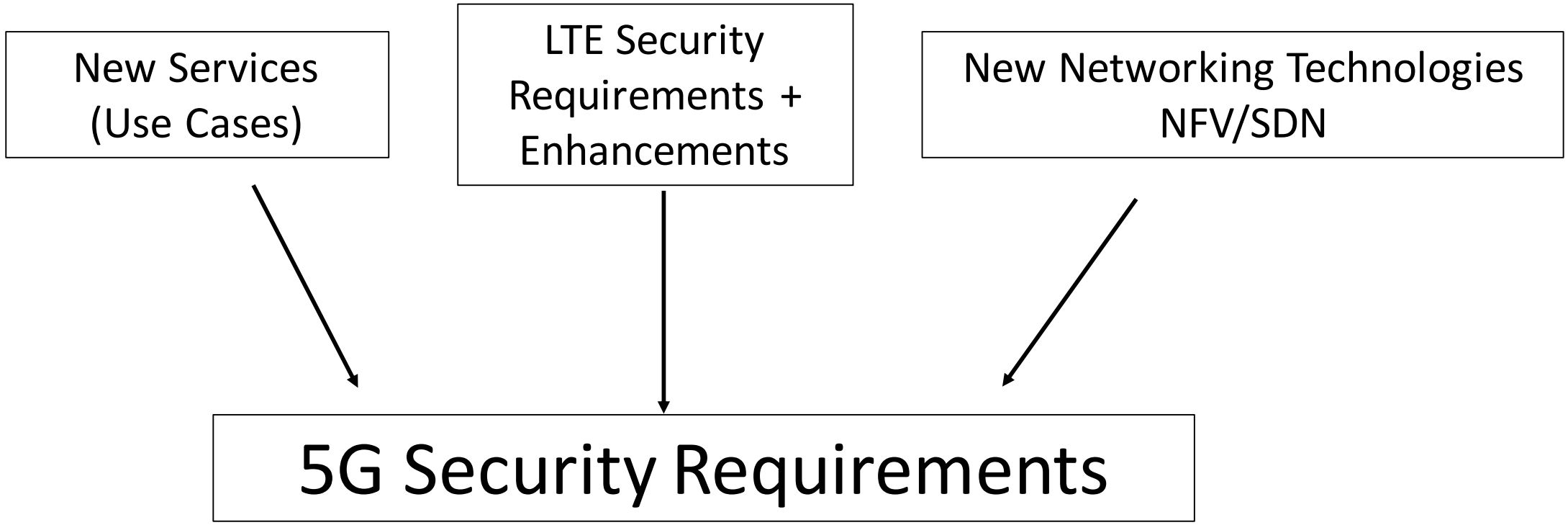
HITB GSEC 2019, Singapore

5G?

Human Communication

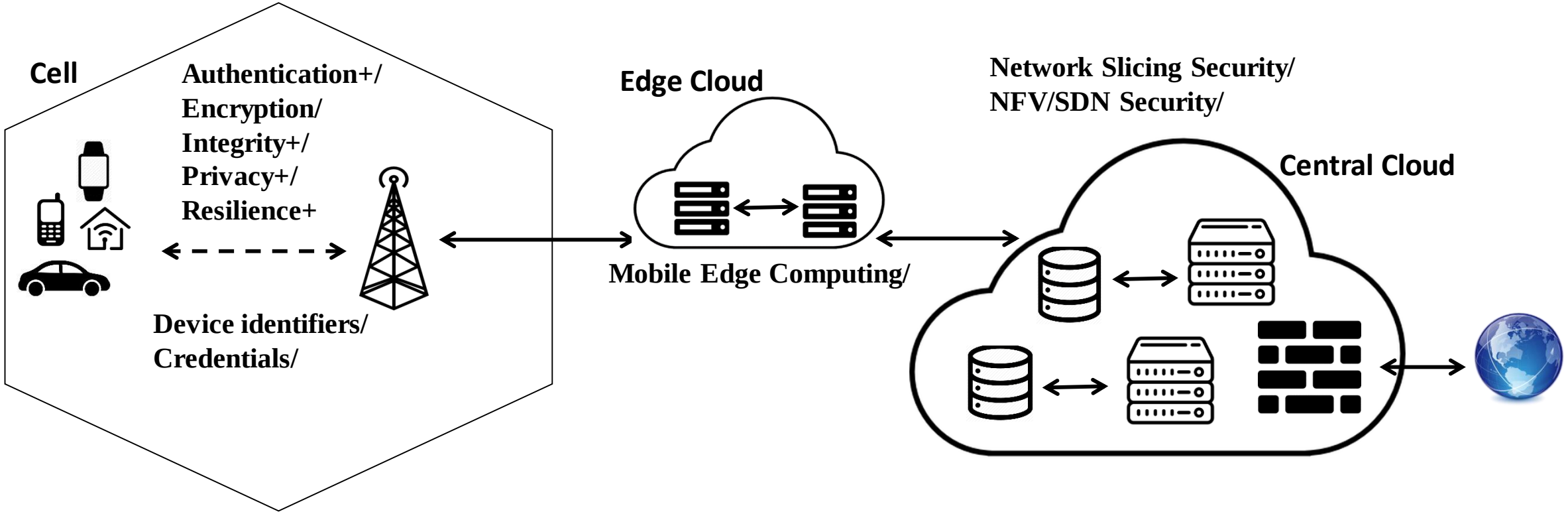
Machine Communication

5G Sec.?



Source: https://www.informationsecuritybuzz.com/articles/security-challenges-next-generation-5g-mobile-networks/

5G Security Elements



Security Evolution (OTA)

Phone

no mutual authentication **2G**

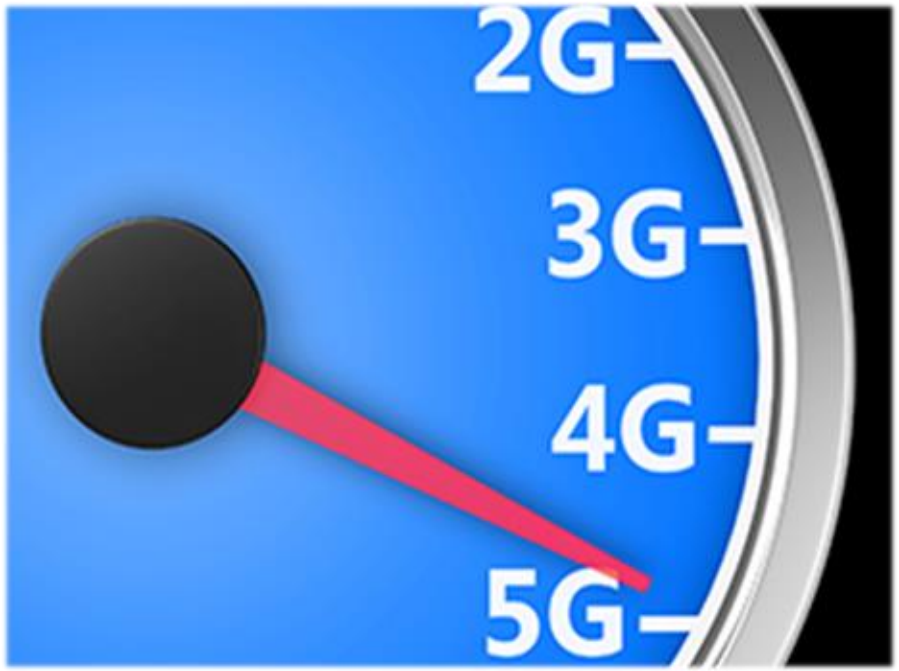
mutual authentication
integrity protection **3G**

mutual authentication
deeper mandatory integrity protection **4G**

mutual authentication ++
deeper mandatory protection features++ **5G**

Base Station

IMSI Catchers in 5G.?



IMSI IMEI

IMSI IMEI

IMSI IMEI

IMSI IMEI

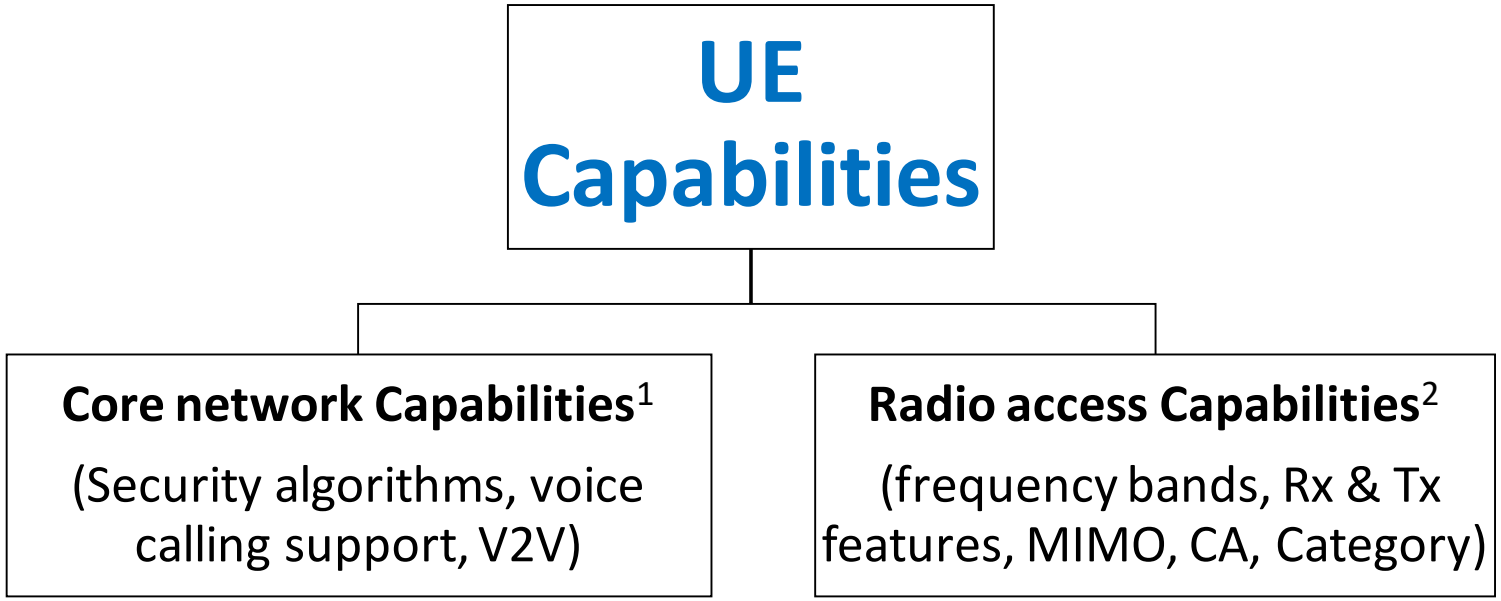
5G Security

- 5G Security **>>** 4G ? (What's new)
- Similar security protocols and algorithms?
- Attacks in 4G/LTE fixed.?
  - Downgrade attacks, DoS attacks, Location tracking
- What's not fixed in 4G – **copy pate** to 5G

Another** IMSI catcher or fake base station attacks in 5G?

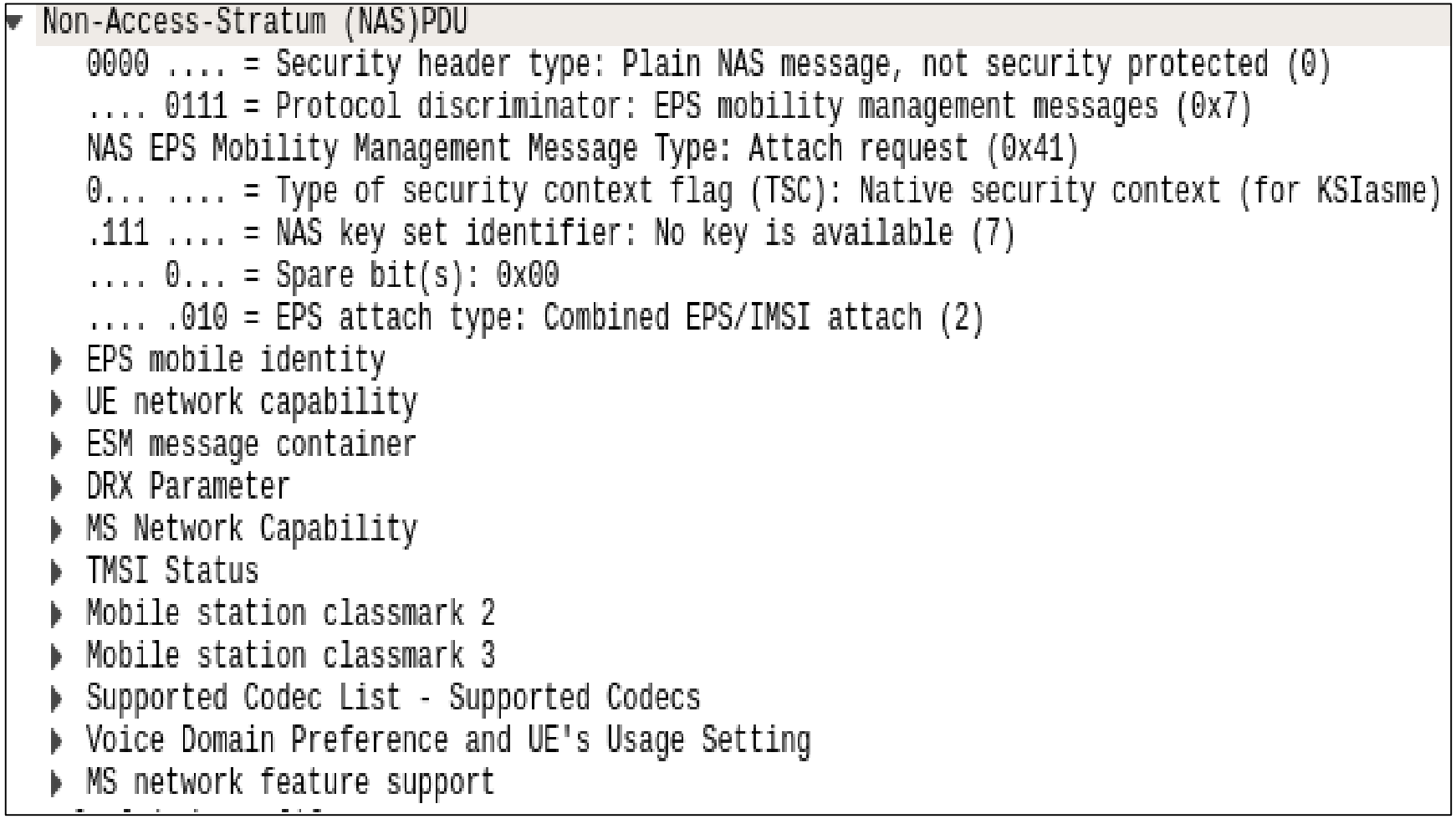
** Ravishankar Borgaonkar, Lucca Hirschi, Altaf Shaik, and Shinjo Park "New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols "
https://eprint.iacr.org/2018/1175

Capabilities?



1. 3GPP TS 24.301, 23.401, 24.008
2. 3GPP TS 36.331

Core Capabilities



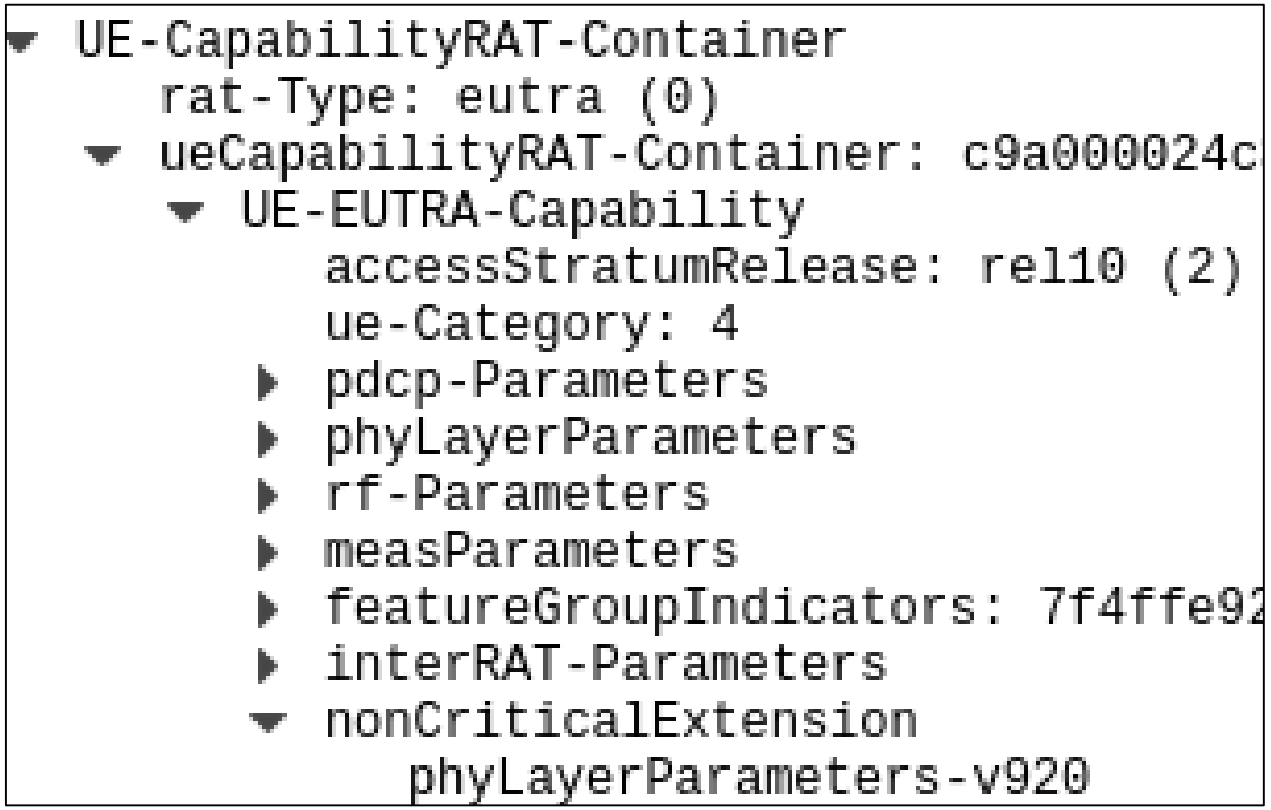
Capabilities 5G

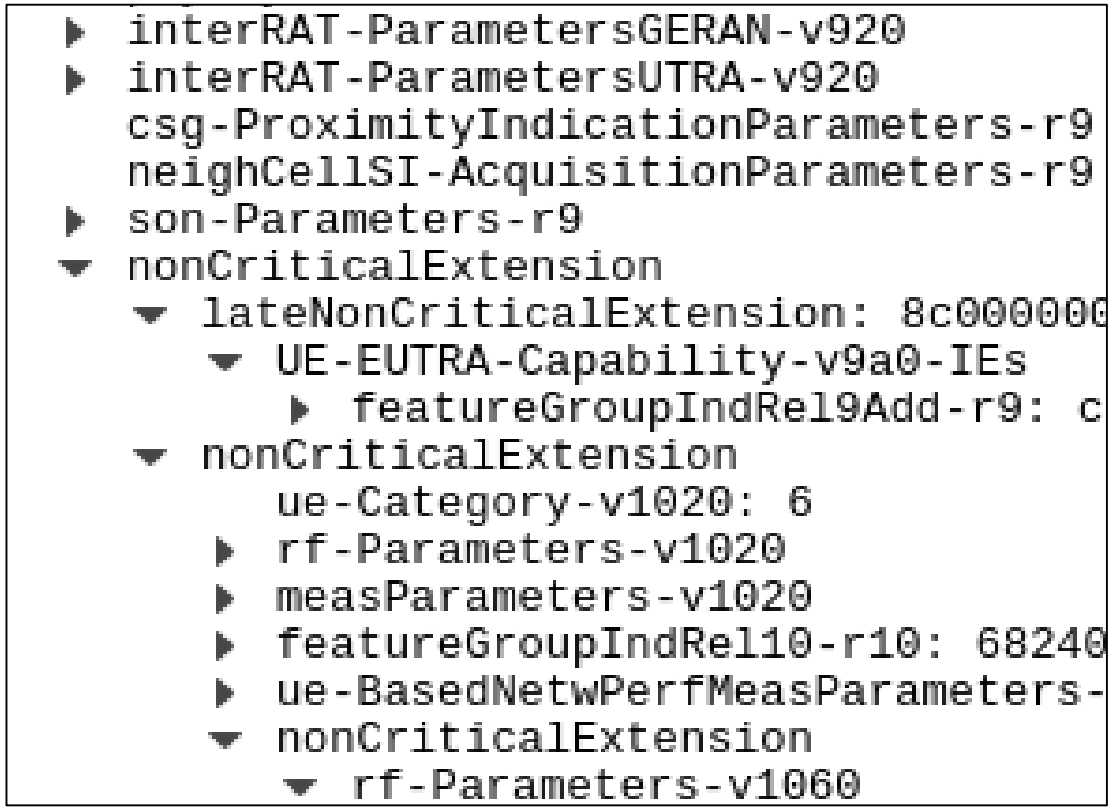
- V2X: Connected Cars
- Prose (D2D): Location services
- CIoT: IoT specific

8	7	6	5	4	3	2	1	
UE network capability IEI								octet 1
Length of UE network capability contents								octet 2
EEA0	128-EEA1	128-EEA2	128-EEA3	EEA4	EEA5	EEA6	EEA7	octet 3
EIA0	128-EIA1	128-EIA2	128-EIA3	EIA4	EIA5	EIA6	EIA7	octet 4
UEA0	UEA1	UEA2	UEA3	UEA4	UEA5	UEA6	UEA7	octet 5*
UCS2	UIA1	UIA2	UIA3	UIA4	UIA5	UIA6	UIA7	octet 6*
ProSe-dd	ProSe	H.245-ASH	ACC-CSFB	LPP	LCS	1xSRVCC	NF	octet 7*
ePCO	HC-CP CIoT	ERw/o PDN	S1-U data	UP CIoT	CP CIoT	Prose-relay	ProSe-dc	octet 8*
15 bearers	SGC	N1mode	DCNR	CP backoff	RestrictEC	V2X PC5	multipleDRB	octet 9*
0	0	0	0	0	0	0	0	octet 10* - 15*
Spare								

Figure 9.9.3.34.1: UE network capability information element

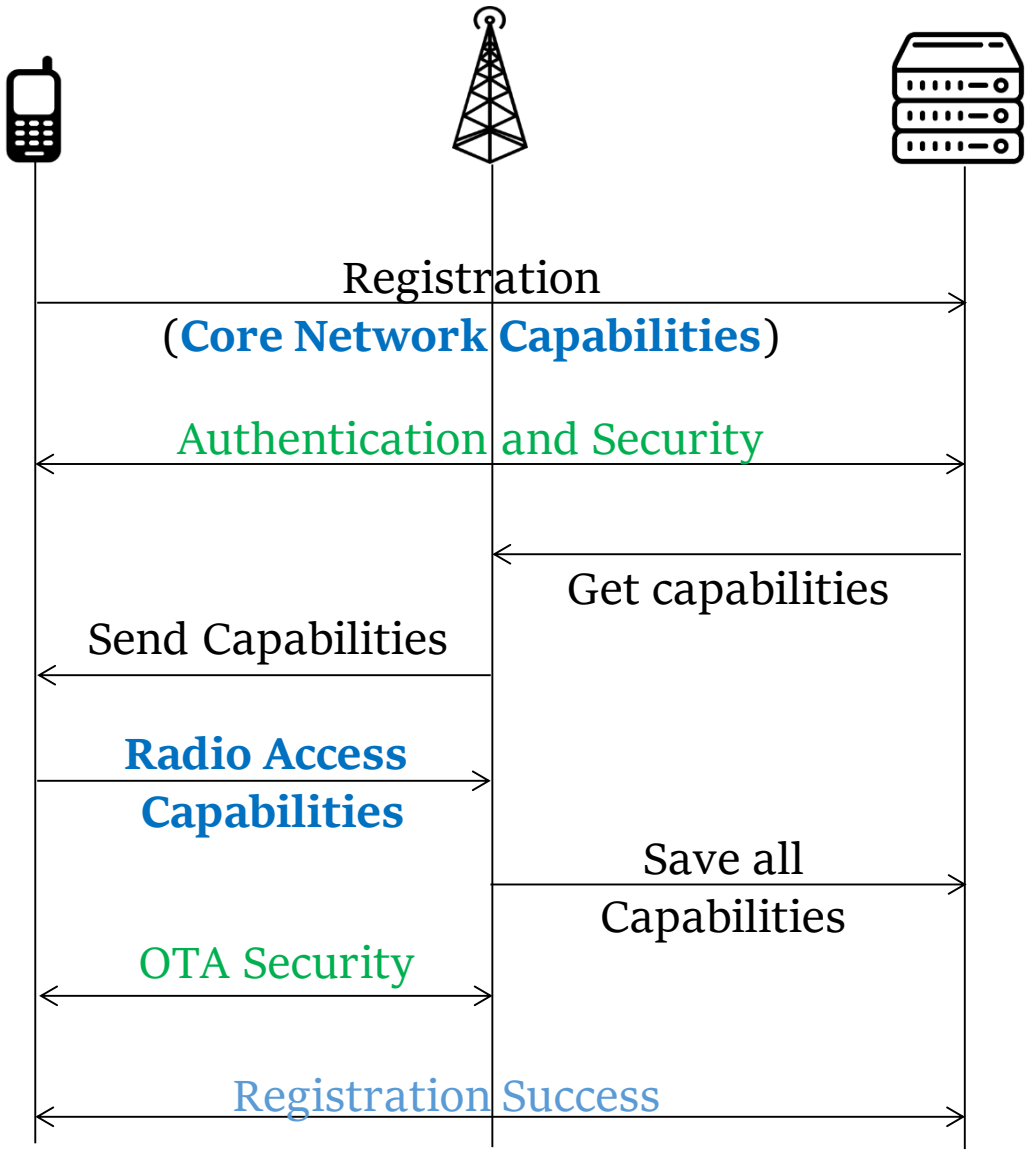
Radio Capabilities





LTE Registration

- UE Capabilities
  - sent to network while registration
  - stored at network for long periods
  - **visible in plain-text over-the-air**
    - **Passive and active attacks**



Issue?

UE Capabilities

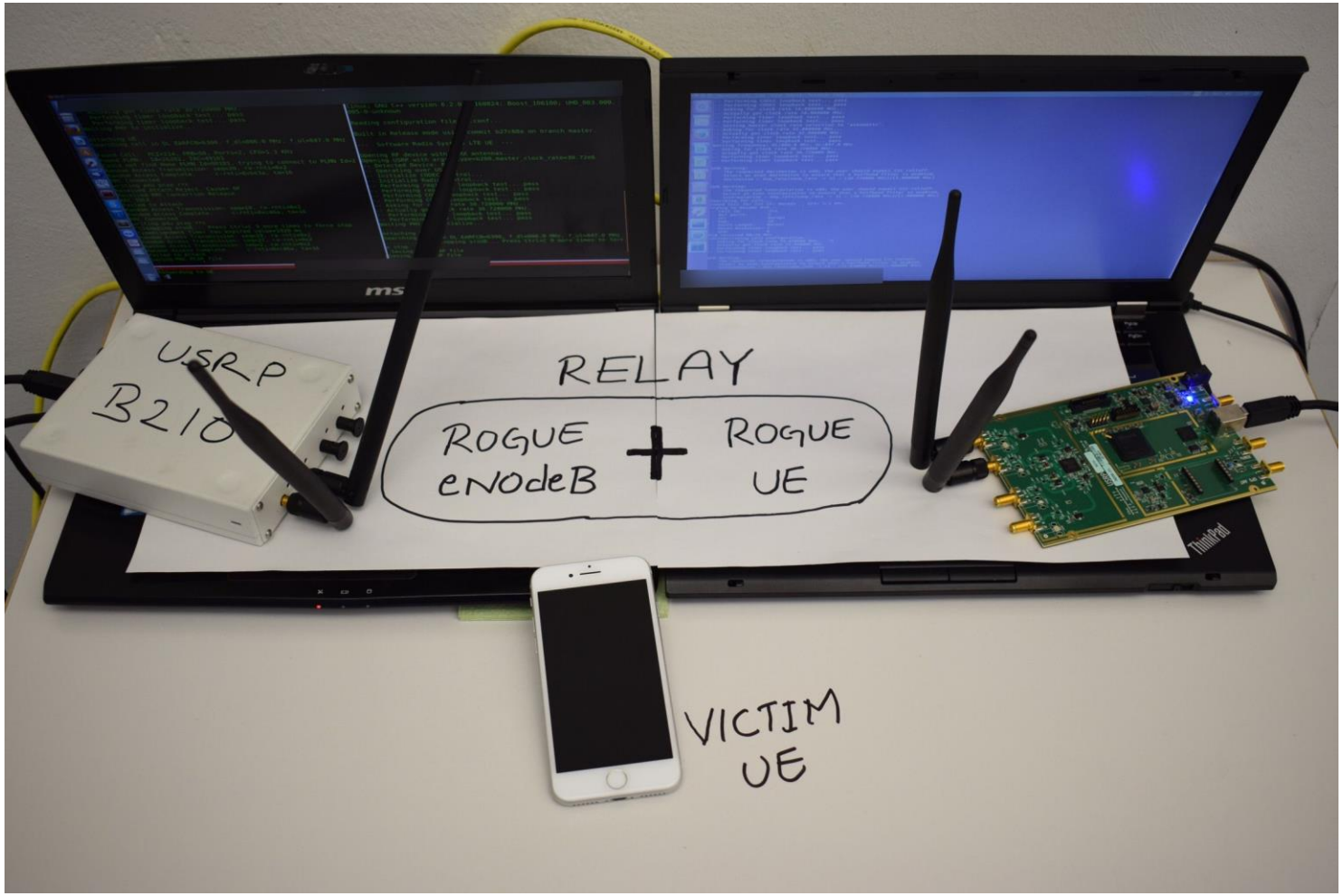
- Accessible by fake base stations
- Sent plain-text over the air
- Standard + Implementation bugs

Attacks?

- **MNmap (active or passive)**
- **Bidding down (MITM)**
- **Battery Drain (MITM)**

Setup – LTE MitM attacker

- Hardware
  - **2 X (USRP B210 + Laptops)**
  - Phones, Quectel modems, cars, IoT devices, trackers, laptops, routers….
- Software
  - **SRSLTE**
- **Attacks tested with real devices and commercial networks**



1. MNmap

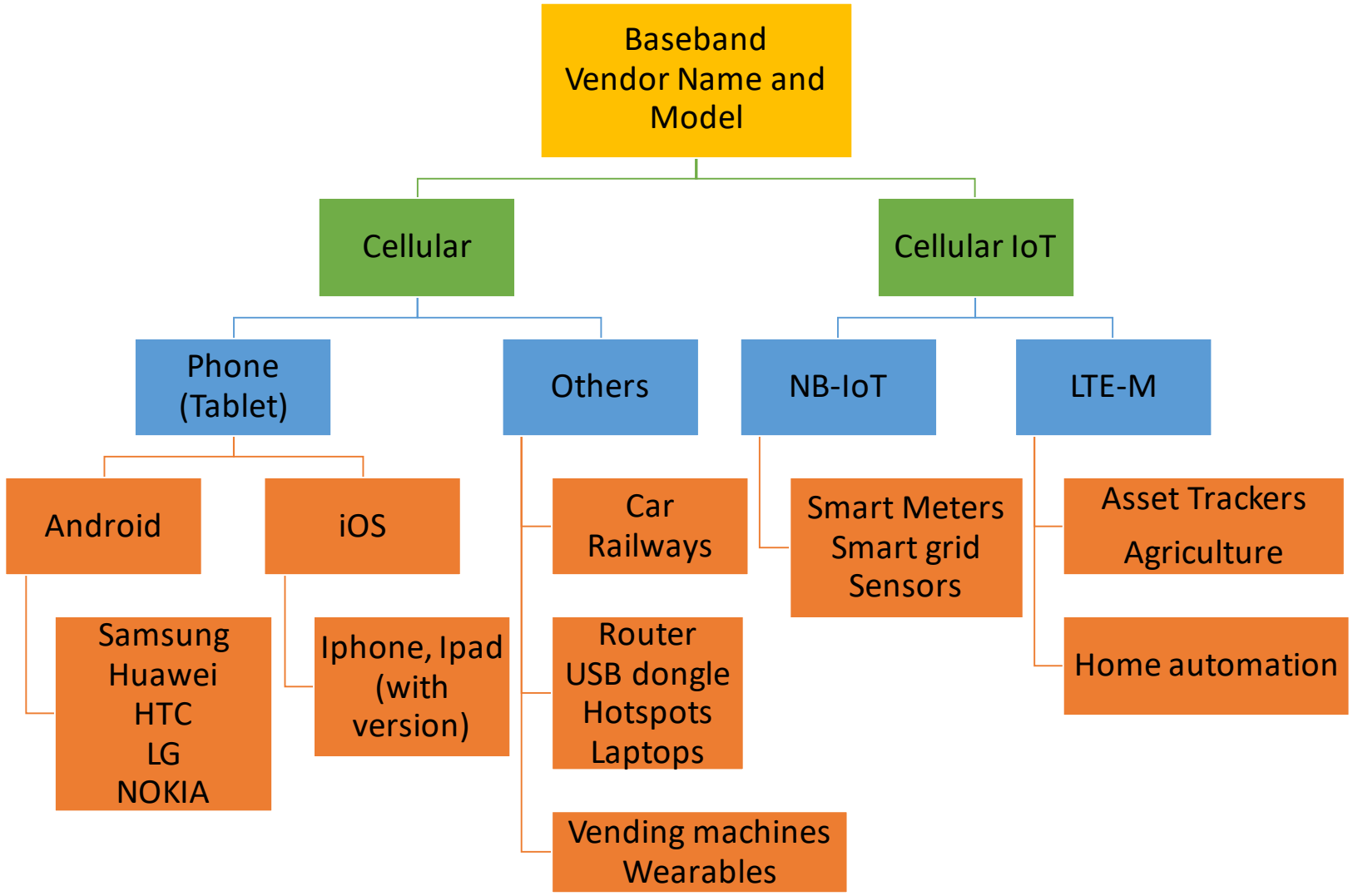
- (**Mobile Network Mapping**)
  similar to IP Nmap

- **Maker**
- **Model**
- **OS**
- **Applications**
- **Version**

1. MNmap

Identify any cellular device in the wild

Chip Maker,
Device Model,
Operating System,
Application of device,
Baseband Software Version



Identification – How

Baseband vendors implement capabilities differently

- For e.g., Qualcomm Chipsets always Disable EAI0
- Many Capabilities are **optional**, (disabled/enabled)

Each target application requires different set of UE Capabilities

- V2V for automated car
- Voice calling and codec support for phone
- GPS capability for tracker
- Data only support for routers, USB data sticks (SMS only)

Devices Under Tests

Manufacturer	Model	Baseband Type
Samsung	Galaxy Alpha	Intel XMM7260
Samsung	Galaxy S6	Samsung Exynos Modem 333
Samsung	Galaxy S7	Samsung Exynos 8890
Samsung	Galaxy S8	Samsung Exynos 8895
Huawei	Honor 7	Kirin 935
Huawei	P20	Kirin 970
HTC	One E9	MediaTek X10
LG	G Flex 2	Qualcomm MSM8994
Sony	Xperia Z5	Qualcomm MSM8994
Sony	Xperia X	Qualcomm MSM8956
Planet Computer	Gemini	MediaTek X27
Apple	iPhone 6	Qualcomm MDM9625
Apple	iPhone 8	Intel XMM7480
Apple	iPhone 8 (US)	Qualcomm MDM9655
Apple	iPhone X (US)	Qualcomm MDM9655
Google	Nexus 5X	Qualcomm MSM8992
Nokia	8110 4G	Qualcomm MSM8905
Asus	ZenFone 2E	Intel XMM7160

Manufacturer	Model	Baseband Type
Huawei	E3372	Huawei
Samsung	GT-B3740	Samsung CMC220
Sierra Wireless	EM7455	Qualcomm MDM9635
Fibocom	L850-GL	Intel XMM7360
Telit	LN930	Intel XMM7160
AVM	FritzBox LTE	Intel XMM7160
Huawei	B310s	Huawei
Netgear	Nighthawk	Qualcomm MDM9250
GlocalMe	G2	Qualcomm MSM8926
Quectel	BC68	Huawei NB-IoT
Quectel	BC66	MediaTek NB-IoT
Quectel	BG69	Qualcomm MDM9206
Audi	A6	Qualcomm MDM9635
Samsung	SM-V110K	Qualcomm MDM9206
Mobile Eco	ME-K60KL	Qualcomm MDM9206
Apple	Watch Series 3	Qualcomm MDM9635M
Huawei	MediaPad M5	Kirin 960
Apple	iPad 5th gen	Qualcomm MDM9625M

Ref model

Devices

- Baseband vendor
- Application
- Chipset name
- 3GPP release

Fingerprints

Implementation differences among Baseband vendors

Capability	Huawei	Samsung	Intel	Mediatek	Qualcomm
CM Service Prompt	1	0	0	0	1
EIA0	1	1	1	1	0
Access class control for CSFB	0	1	0	1	1
Extended Measurement Capability	0	0	0	1	0

Chipset info

List of Qualcomm Snapdragon

From Wikipedia, the free encyclopedia

This is a list of Qualcomm Snapdragon chips. Snapdragon is a for use in smartphones, tablets, and smartbook devices.

Contents [hide]

HiSilicon

From Wikipedia, the free encyclopedia

HiSilicon (Chinese: 海思; pinyin: *Hǎisī*) is a Chi

HiSilicon purchases licenses for CPU designs fr MPCore, ARM Cortex-A15 MPCore,[2][3] ARM C licenses from Vivante Corporation for their GC4

HiSilicon is reputed to be the largest domestic d

Contents [hide]

MediaTek

From Wikipedia, the free encyclopedia

This article appears to cor article if you can. *(February*

MediaTek Inc. (Chinese: 聯發科技股份有限公司; pinyin: *Lián* for wireless communications, High-definition television, hanc multimedia products and Digital subscriber line services as v

Headquartered in Hsinchu, Taiwan, the company has 25 offi in 1997, MediaTek has been creating chipsets for the global

Contents [hide]

Exynos

From Wikipedia, the free encyclopedia

This acce

Exynos (from the Greek words exyp developed and manufactured by San

Contents [hide]

Half-way

1. Baseband Maker
2. Baseband Model
3. List of supported devices for the chipset
4. Identify the right device and application

Fingerprints

Difference b/w phone and other devices

Capability	Phone	Others
UE's Usage setting	Voice or Data	Not present
Voice domain preference	CS Voice or PS Voice	Not present
UMTS AMR codec	Present	Not

Phone and preferred Baseband

Phone	Baseband
Huawei	Huawei
Samsung	Samsung
Apple	Intel or QCT

Difference b/w iOS and Android

Capability	Android	iOS
MS assisted GPS	1	0
Voice over PS-HS-UTRA-FDD-r9	1	0

Difference b/w cellular and cellular IoT

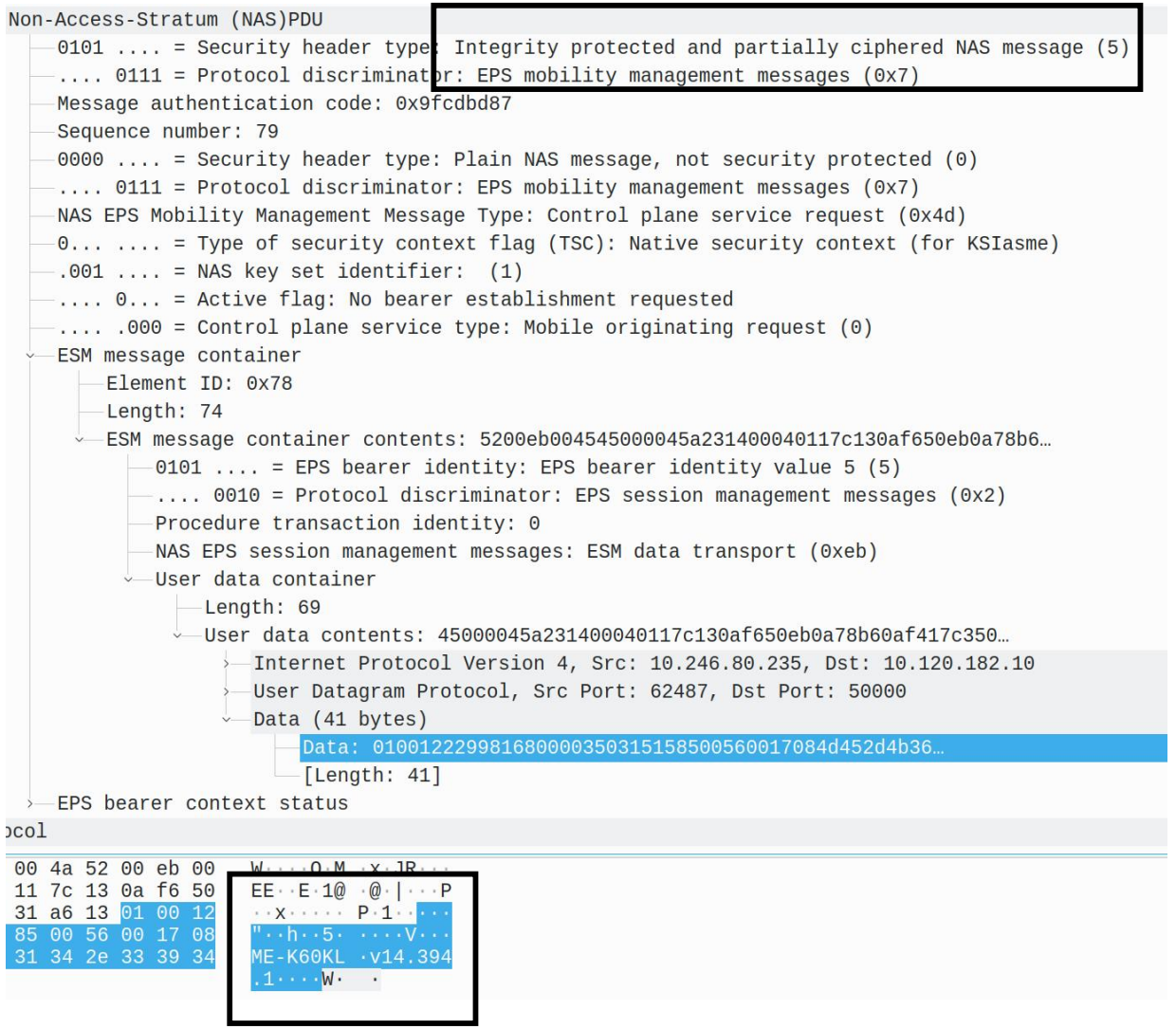
Capability	Cellular IoT	Cellular
PSM Timer	1	0
T3412 ext period TAU timer	1	0

MNmap issues

- SIM card can have affect on capabilities
  - enabled/disabled – operator setting, e.g., bands
- IoT applications LTE-M vs NB-IoT
  - Timer values (low for smart meters, high for asset trackers)
- Success and failures in detecting (close to round off, multiple options)

Zero Encryption for IoT

- **Integrity protected and partially ciphered**
- **EEA0 for NAS by some X operator**
- **IoT devices depend on Air interface security**
- **Device details in clear**

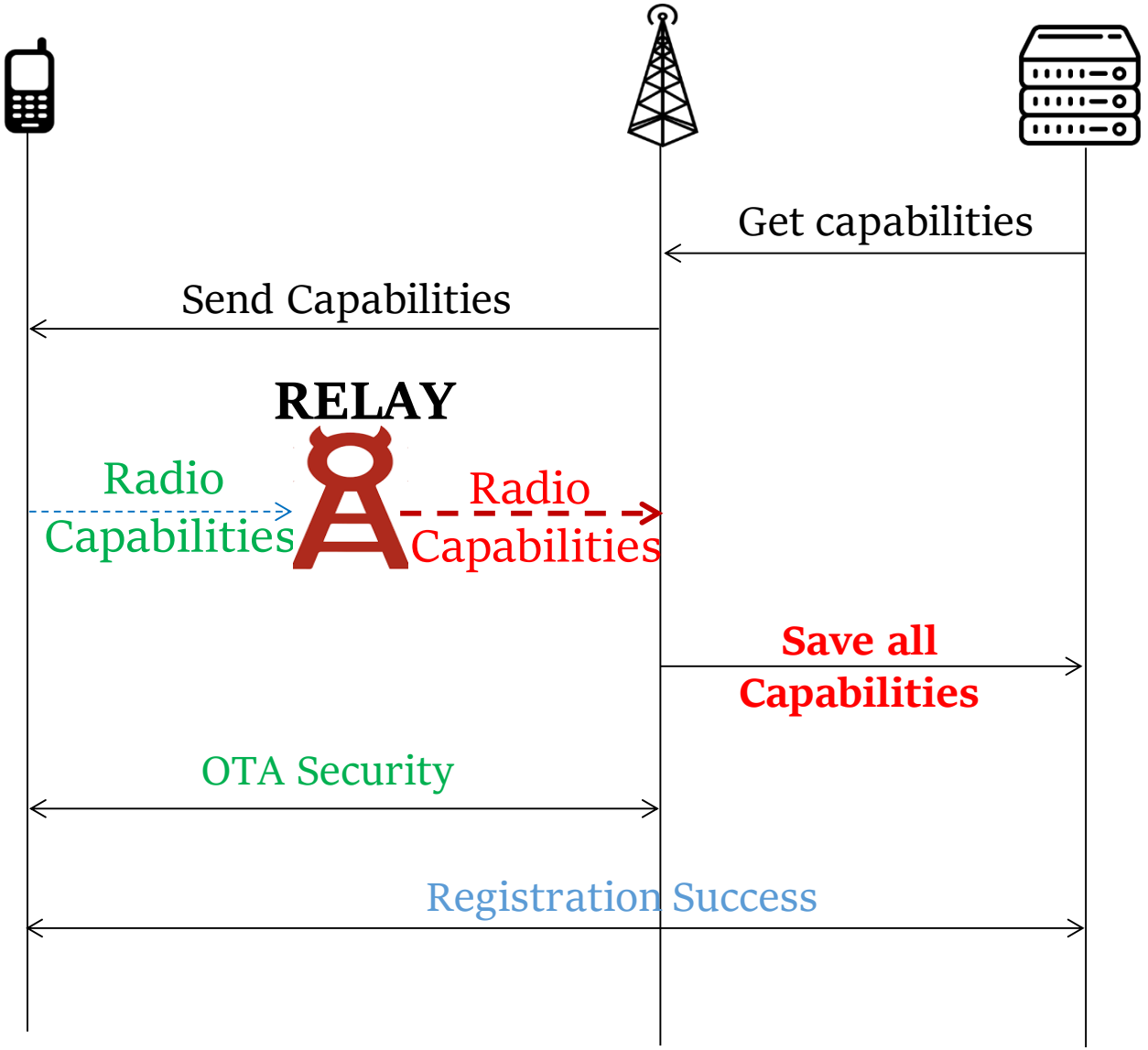


What next

- Passive MNmap also works (active base station not required)
- Privacy
  - Link IMSI to device capabilities on 4G
    - (associate device fingerprints to people)
- Launch target specific attack
- Open source MNmap : share traces and automated tool

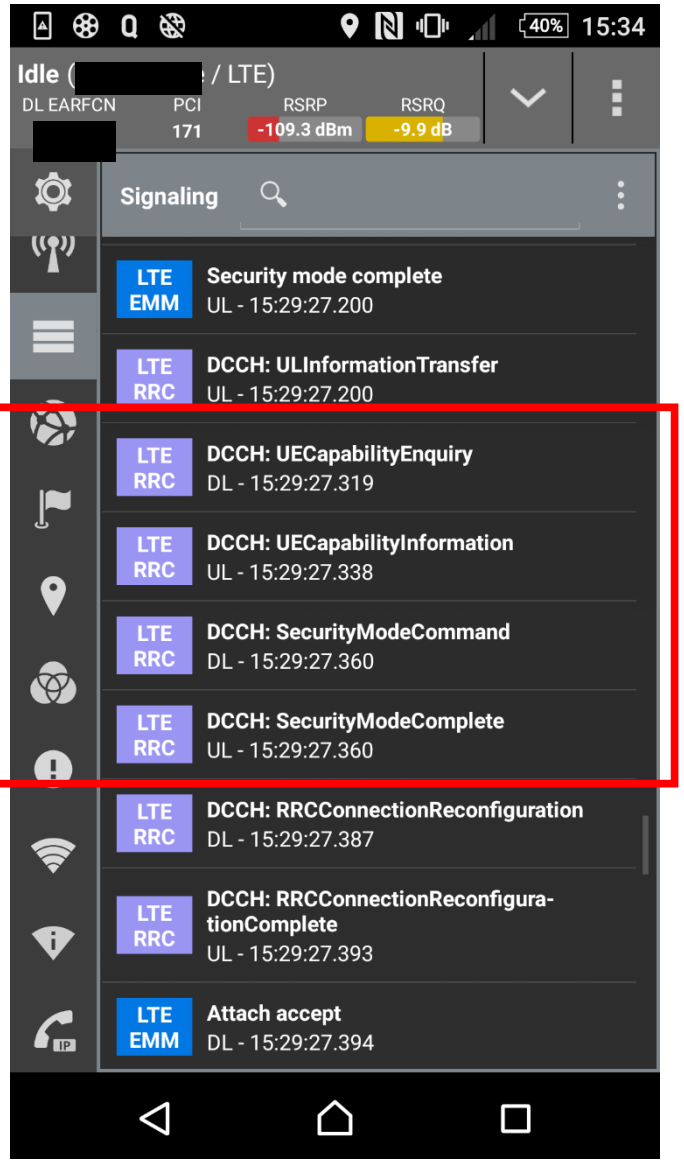
2. Bidding down

- Hijacking
  - Radio Capabilities
  - MitM relay before OTA Security
  - Network/Phone cannot detect



Bidding down

- Radio Capabilities are modified
  - UE Category changed (Cat 12 -> Cat 1)
  - CA and MIMO are disabled
  - Frequency Bands are removed
  - VoLTE mandatory requirements are disabled
  - V2V capabilities can be removed



Tests with real networks

- LTE service downgrade (with elite USIM)
  - Iphone 8 and LTE Netgear router (Qualcomm Basebands)
  - Data Rate (downlink) 48 Mbps to 2 Mbps (USA and Europe)
  - VoLTE calls are denied to UE (CSFB used)
  - Handovers to 2G/3G due to lack of band support – downgraded

Impact

- **22 out of 32** tested LTE networks worldwide (Europe, Asia, NA) are affected (USA, Switzerland, France, Japan, Korea Netherlands, UK, Belgium, Iceland etc.)

- Persistent for 7 days
  - Capabilities are **cached** at the Core Network components
  - **Restart** device for normal operation

- **Radio is a bottleneck for high-speed data services

Why without/before Security

3GPP TR 33.809 V0.2.0 (2019-02)

5.1 Key Issue #1: Security of unprotected unicast messages

5.1.1 Key issue details

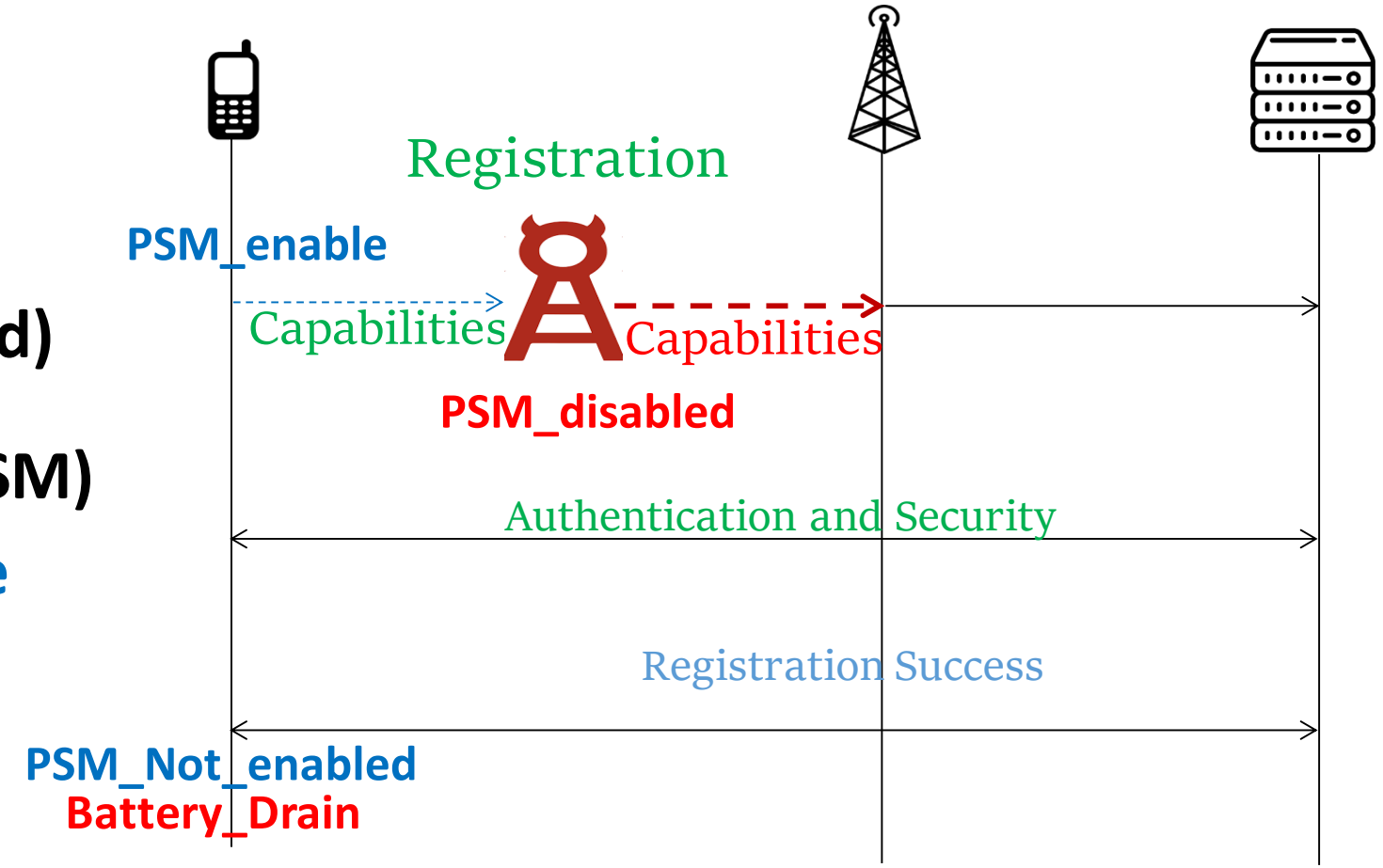
This key issue covers both the uplink and downlink unicast message which could be sent unprotected. An example of unprotected uplink message is RRC UECapabilityInformation, and examples of unprotected downlink messages are RRC UECapabilityEnquiry, and REJECTs in RRC/NAS layers.

In current 3GPP standards, it has been a design choice to allow RRC UECapabilityEnquiry and RRC UECapabilityInformations messages to be sent unprotected "before" AS security activation. The reason for allowing that is to enable the network to do early optimization for better service/connectivity. It means that during the RRC

***To do early optimization for better service/connectivity

3. Battery Drain

- **NB-IoT (Narrow Band)**
- **Power Saving Mode (PSM)**
  - **OFF when not in use**



Tests

- **PSM disabled (UE and network don't detect)**
- Continuous activity - Neighbor cell measurements
  - **drains battery (10 year battery??)**
- Experiment with NB-IoT UE (Quectel BC68 modem)
  - Reconnects after 310 hours (13 days)
  - **Battery lifetime reduced by 5 times**
- Persistent attack: restart required to restore

Vulnerability Status & Impact

- Responsibly reported to GSMA, 3GPP SA3, & other affected operators /vendors
- Thanks to GSMA: findings verified (CVD-2019-0018) & SA3 to add fixes
- Core network capabilities are still unprotected
  - MNmap still possible on 5G : passive, active

GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Mobile Security Hall of Fame

SA3 will update 33.501 and 33.401 with a requirement that:

The network should run the RRC UECapabilityEnquiry procedure only after AS security has been activated.

Fixes for Deployed 4G/5G Networks

- ✓ Fixes in LTE release 14 for NB-IoT will appear commercially soon in the devices

- ✓ UE Capabilities should be security protected : accessible only after mutual authentication
  - Operators eNodeB implementation/configuration should be updated

- ✓ Capabilities should be replayed to UE after NAS security setup for verification – Hash of them
  - V2V, Voice calling features, PSM timers, etc.

Thank you

altaf329@sect.tu-berlin.de
ravi.borgaonkar@sintef.no
Director@kaitiaki.in