New Vulnerabilities in 5G Networks

Altaf Shaik
(Technische Universität Berlin, Germany)

Ravishankar Borgaonkar
(SINTEF Digital, Norway)

Blackhat 2019, USA

Identity catching

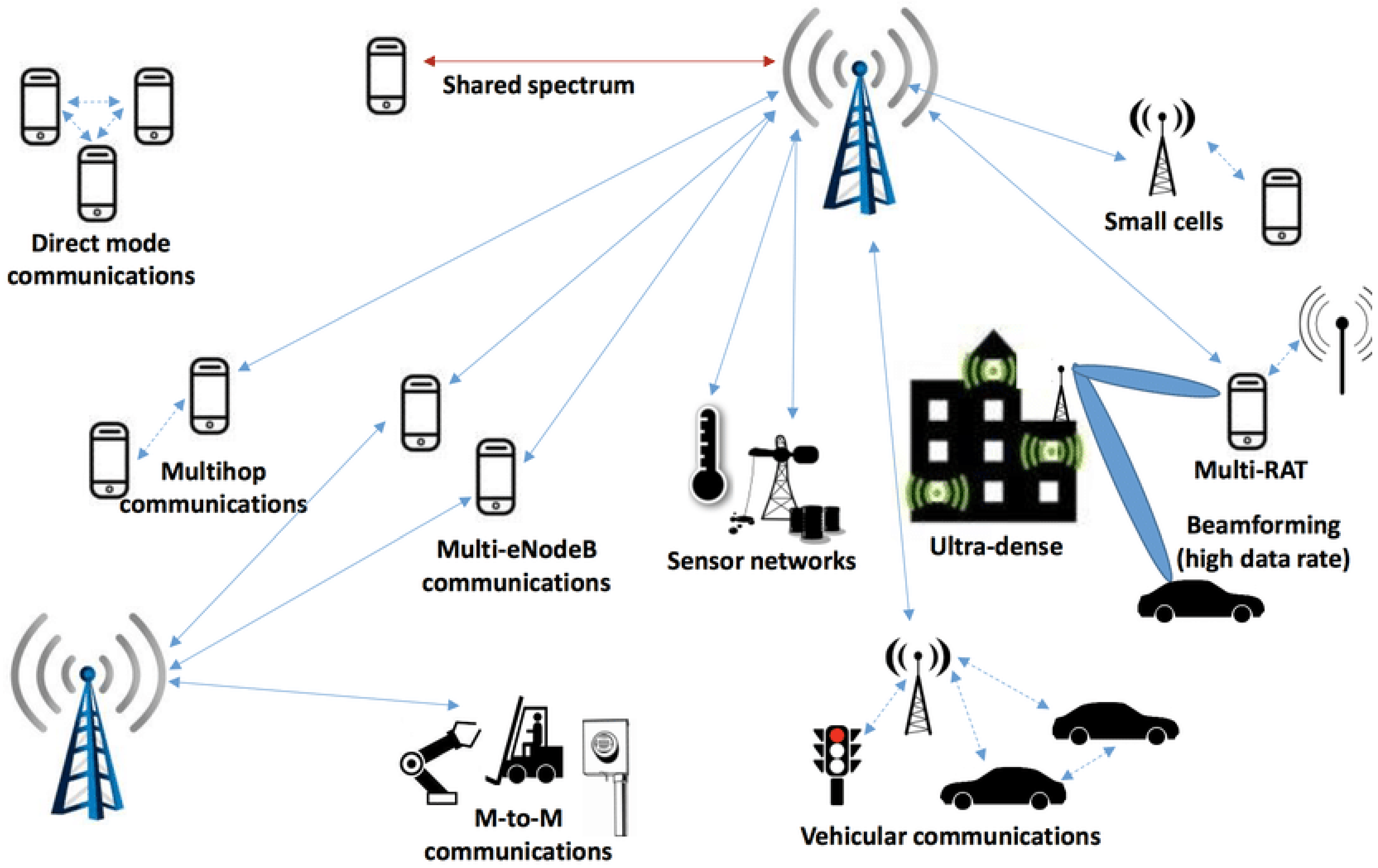
IMSI IMEI

IMSI IMEI

IMSI ~~IMEI~~

~~IMSI~~ ~~IMEI~~

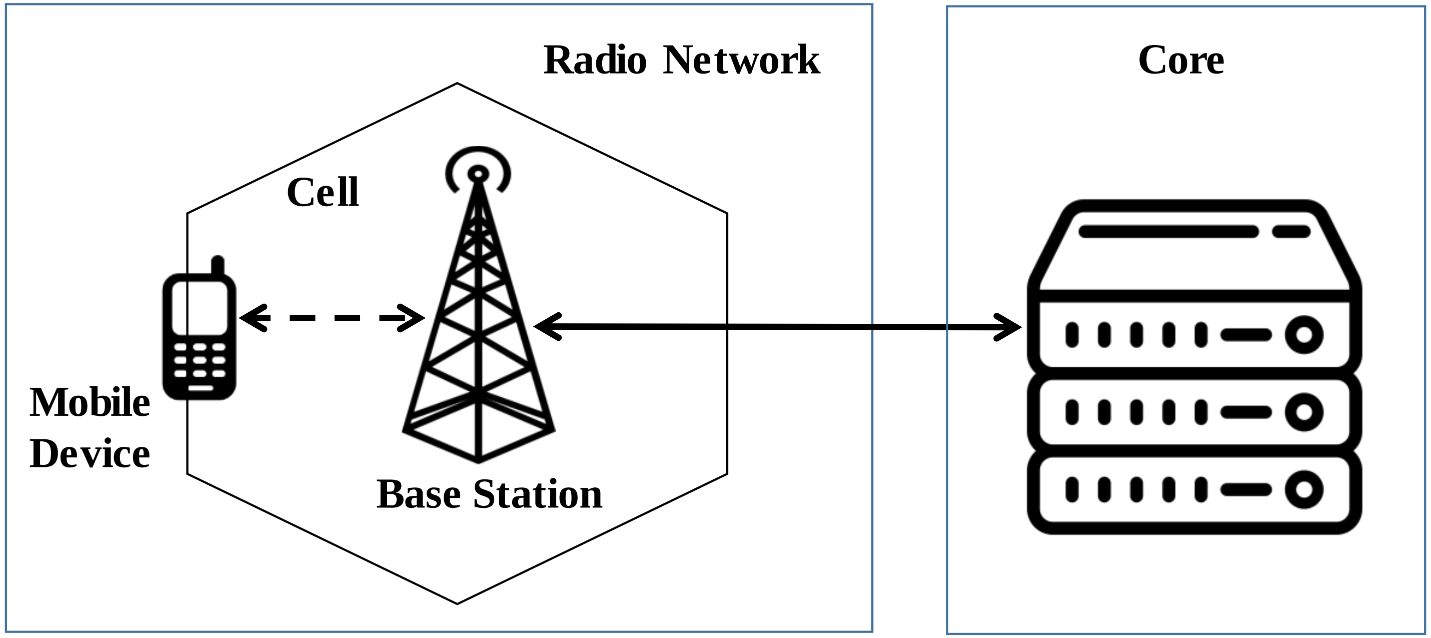
5G?


Shared spectrum
Direct mode communications
Small cells
Multi-RAT
Beamforming (high data rate)
Multihop communications
Multi-eNodeB communications
Sensor networks
Ultra-dense
M-to-M communications
Vehicular communications

5G Security?

- 5G Security **>>** 4G ? (What’s new)
- Same Protocols, Same security algorithms
- Attacks in 4G/LTE fixed.?
    - Downgrade attacks, DoS attacks, Location tracking
- What’s not fixed in 4G – copypaste to 5G

Mobile network



Radio Network

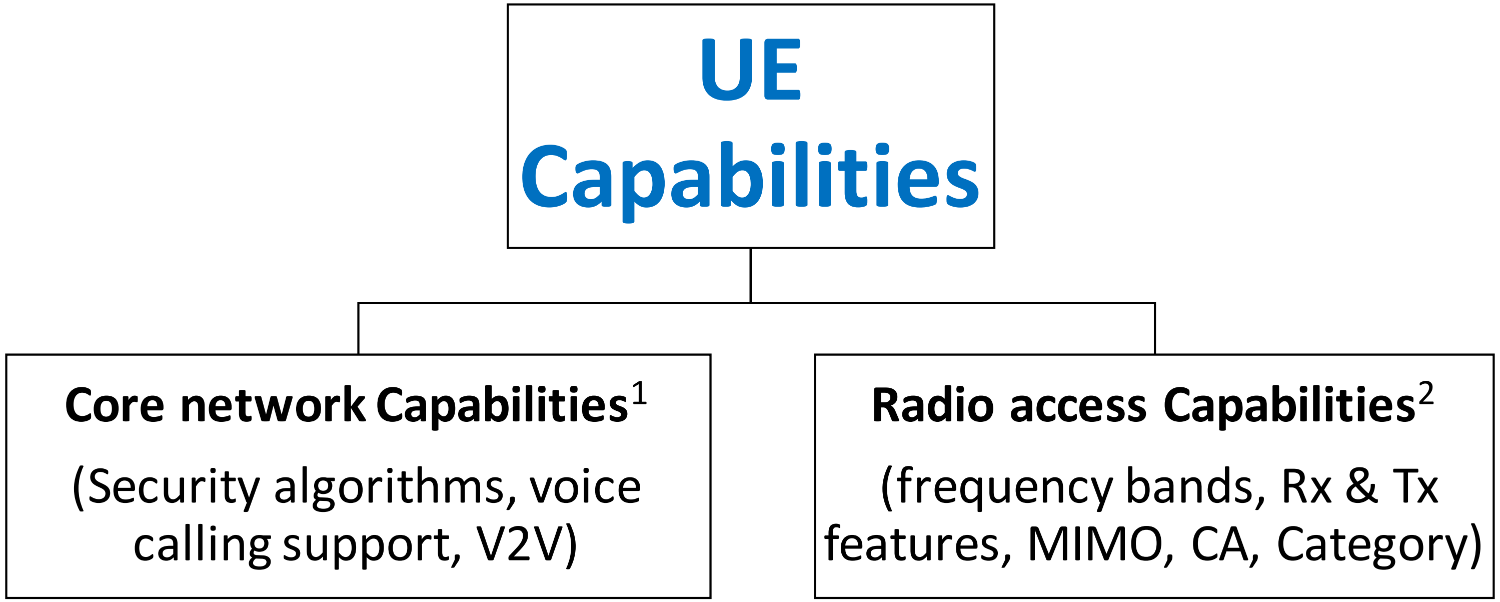
Core

Cell

Mobile Device

Base Station

Capabilities?



UE Capabilities

Core network Capabilities[1]

(Security algorithms, voice calling support, V2V)

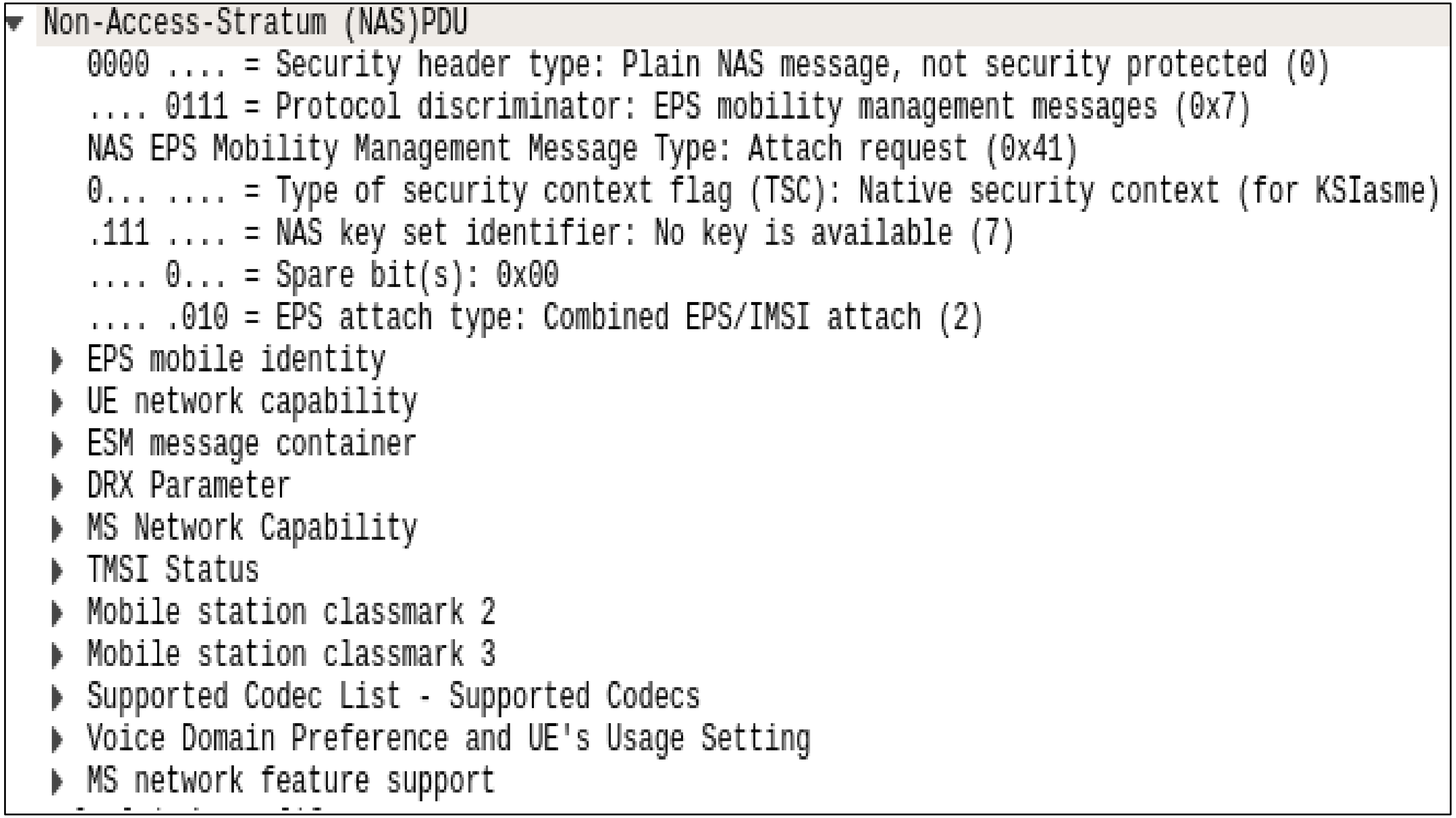
Radio access Capabilities[2]

(frequency bands, Rx & Tx features, MIMO, CA, Category)

[1] 3GPP TS 24.301, 23.401, 24.008

[2] 3GPP TS 36.331

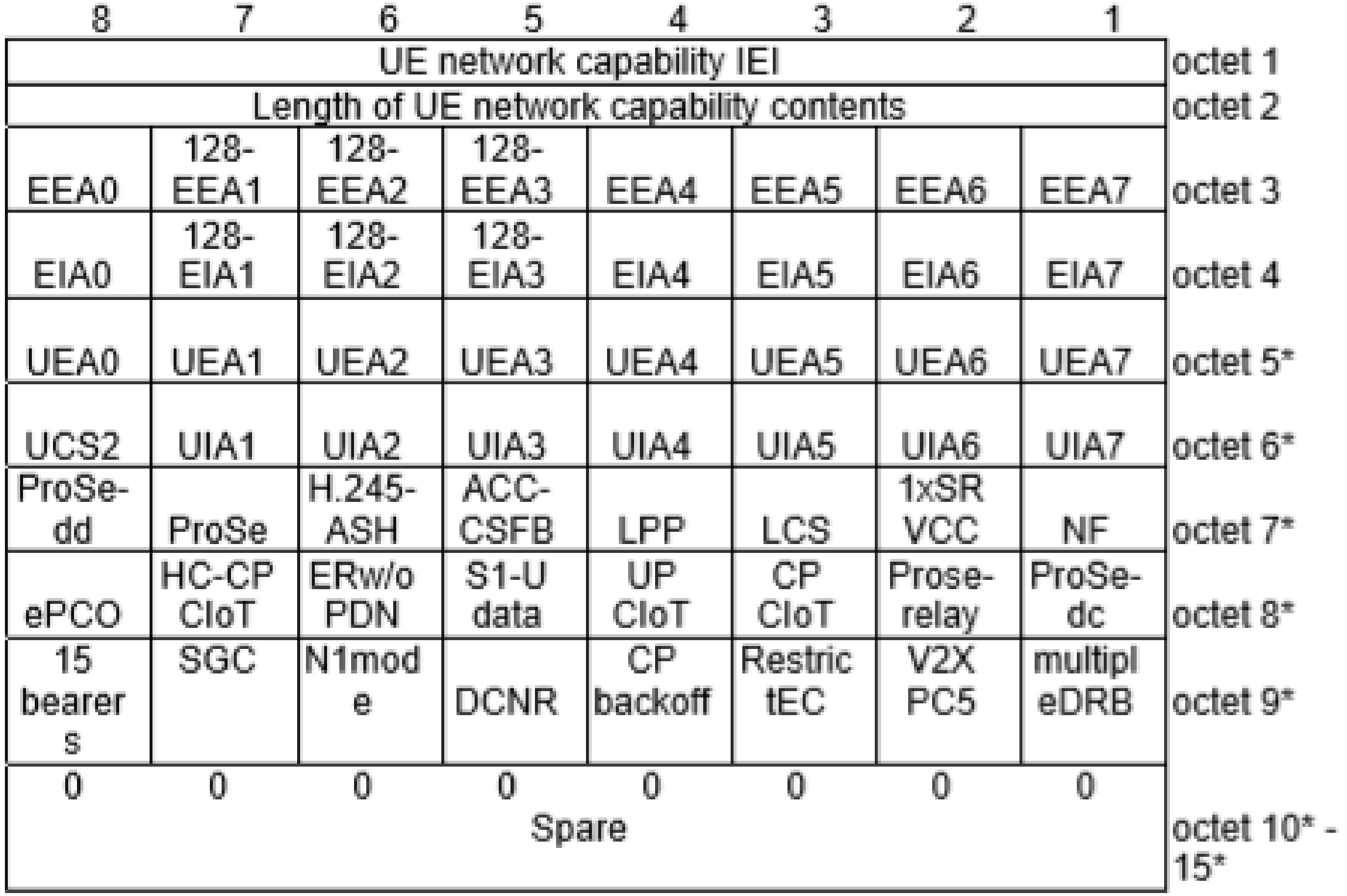
Core Capabilities



```
▼ Non-Access-Stratum (NAS)PDU
     0000 .... = Security header type: Plain NAS message, not security protected (0)
     .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
     NAS EPS Mobility Management Message Type: Attach request (0x41)
     0... .... = Type of security context flag (TSC): Native security context (for KSIasme)
     .111 .... = NAS key set identifier: No key is available (7)
     .... 0... = Spare bit(s): 0x00
     .... .010 = EPS attach type: Combined EPS/IMSI attach (2)
   ▶ EPS mobile identity
   ▶ UE network capability
   ▶ ESM message container
   ▶ DRX Parameter
   ▶ MS Network Capability
   ▶ TMSI Status
   ▶ Mobile station classmark 2
   ▶ Mobile station classmark 3
   ▶ Supported Codec List - Supported Codecs
   ▶ Voice Domain Preference and UE's Usage Setting
   ▶ MS network feature support
```

Capabilities 5G

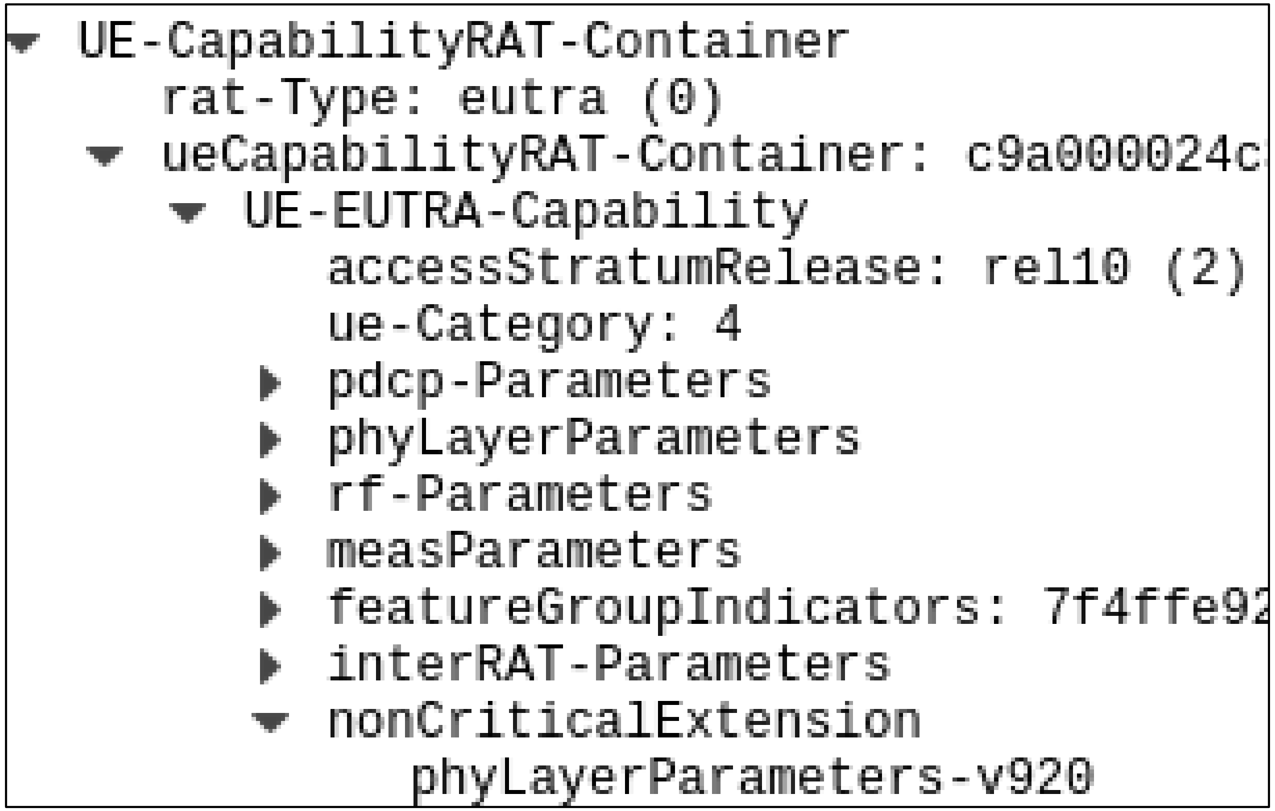
- V2X: Connected Cars
- Prose (D2D): Location services
- CIoT: IoT specific



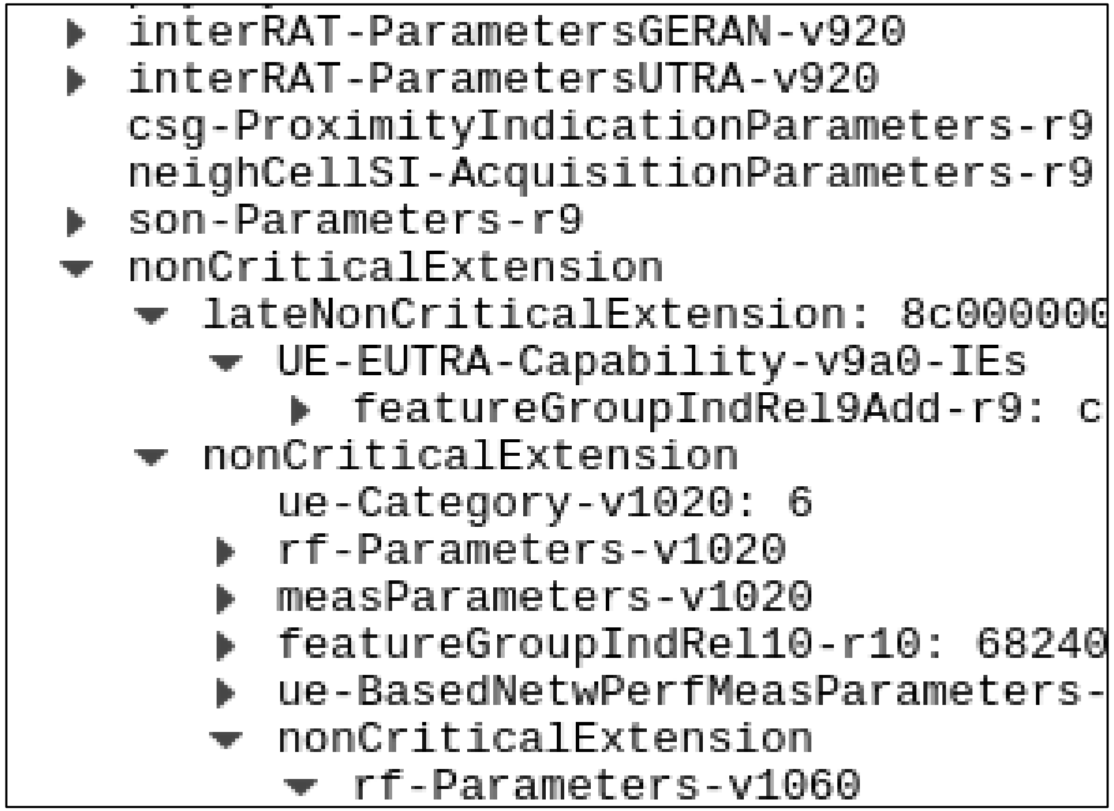
8	7	6	5	4	3	2	1	
UE network capability IEI								octet 1
Length of UE network capability contents								octet 2
EEA0	128-EEA1	128-EEA2	128-EEA3	EEA4	EEA5	EEA6	EEA7	octet 3
EIA0	128-EIA1	128-EIA2	128-EIA3	EIA4	EIA5	EIA6	EIA7	octet 4
UEA0	UEA1	UEA2	UEA3	UEA4	UEA5	UEA6	UEA7	octet 5*
UCS2	UIA1	UIA2	UIA3	UIA4	UIA5	UIA6	UIA7	octet 6*
ProSe-dd	ProSe	H.245-ASH	ACC-CSFB	LPP	LCS	1xSR VCC	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



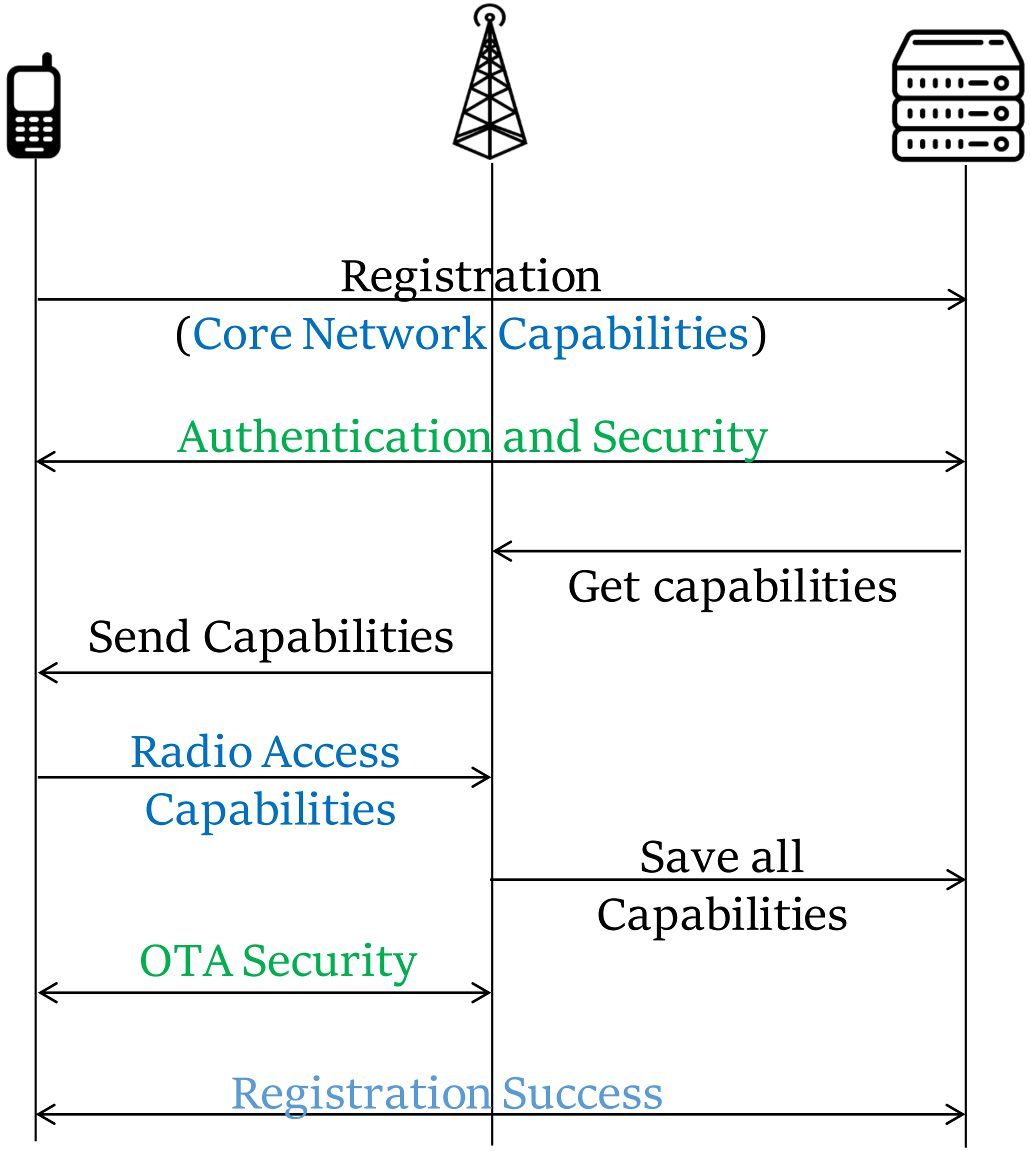
```
▼ UE-CapabilityRAT-Container
    rat-Type: eutra (0)
  ▼ ueCapabilityRAT-Container: c9a000024c
    ▼ UE-EUTRA-Capability
        accessStratumRelease: rel10 (2)
        ue-Category: 4
      ▶ pdcp-Parameters
      ▶ phyLayerParameters
      ▶ rf-Parameters
      ▶ measParameters
      ▶ featureGroupIndicators: 7f4ffe92
      ▶ interRAT-Parameters
      ▼ nonCriticalExtension
          phyLayerParameters-v920
```



```
▶ interRAT-ParametersGERAN-v920
▶ interRAT-ParametersUTRA-v920
  csg-ProximityIndicationParameters-r9
  neighCellSI-AcquisitionParameters-r9
▶ son-Parameters-r9
▼ nonCriticalExtension
  ▼ lateNonCriticalExtension: 8c000000
    ▼ UE-EUTRA-Capability-v9a0-IEs
      ▶ featureGroupIndRel9Add-r9: c
  ▼ nonCriticalExtension
      ue-Category-v1020: 6
    ▶ rf-Parameters-v1020
    ▶ measParameters-v1020
    ▶ featureGroupIndRel10-r10: 68240
    ▶ ue-BasedNetwPerfMeasParameters-
    ▼ nonCriticalExtension
      ▼ rf-Parameters-v1060
```

LTE Registration

- UE Capabilities
  - sent to network while registration
  - Stored at network for long periods
  - **visible in plain-text over-the-air**


Registration (Core Network Capabilities)

Authentication and Security

Get capabilities

Send Capabilities

Radio Access Capabilities

Save all Capabilities

OTA Security

Registration Success

Issue?

UE Capabilities

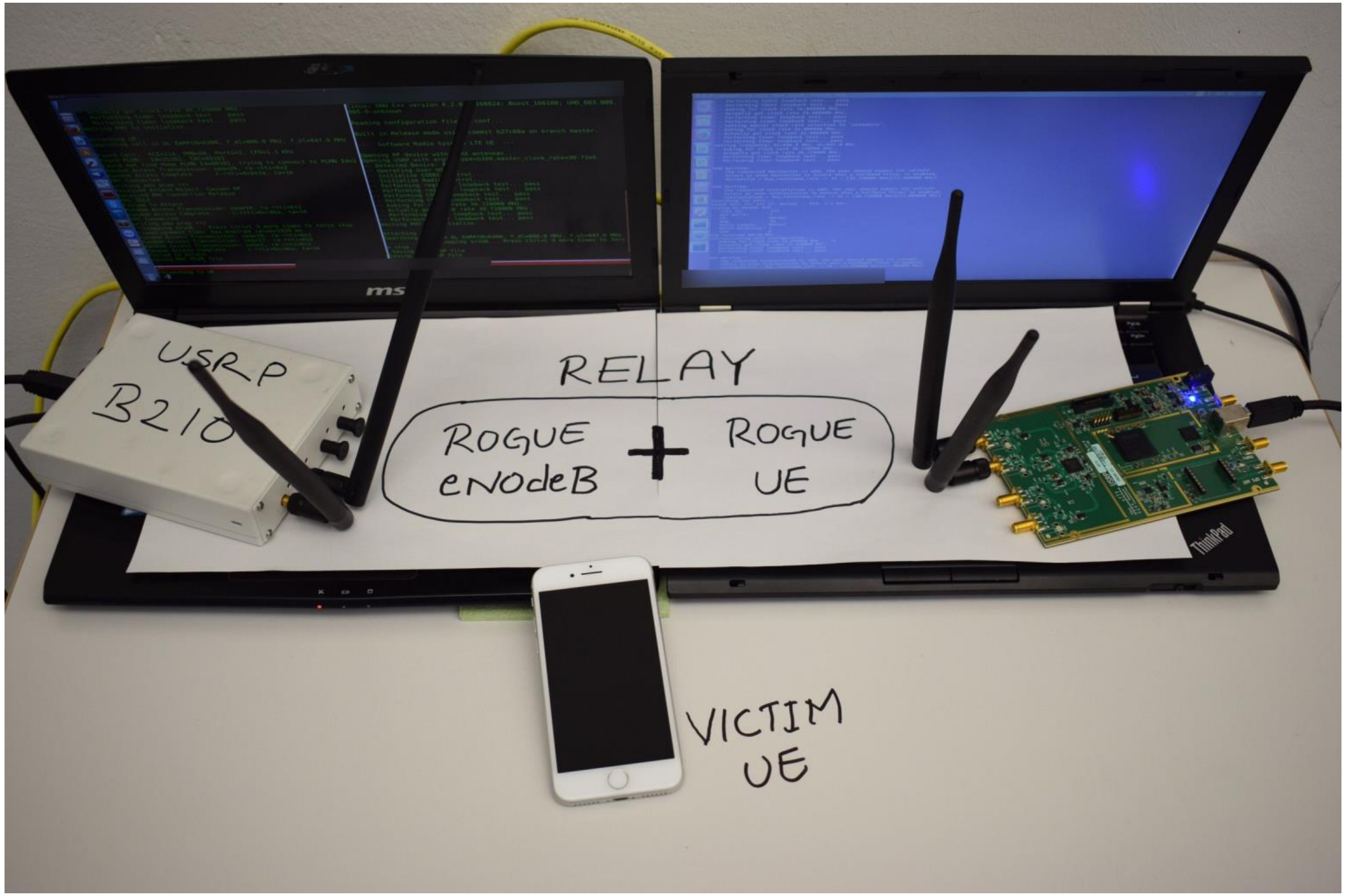
- **Accessible by rogue base stations**
- **Sent plain-text over the air**
- **Standard + Implementation bugs**

Attacks?

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

Setup – LTE MitM attacker

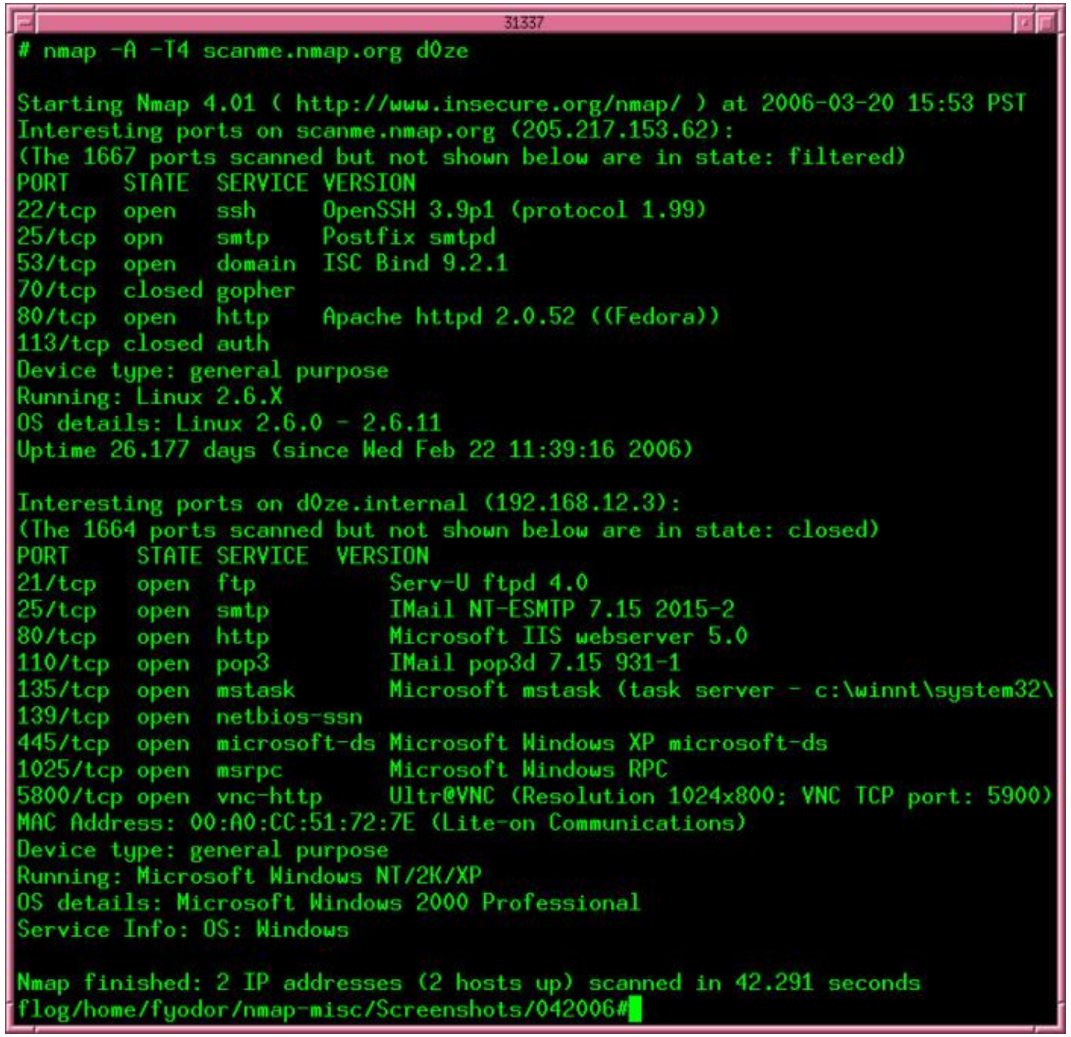
- Hardware
  - **2 X (USRP B210 + Laptops)**
  - Phones, Quectel modems, cars, IoT devices, trackers, laptops, routers….
- Software
  - **SRSLTE**
- **Attacks tested with real devices and commercial networks**



1. MNmap

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

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

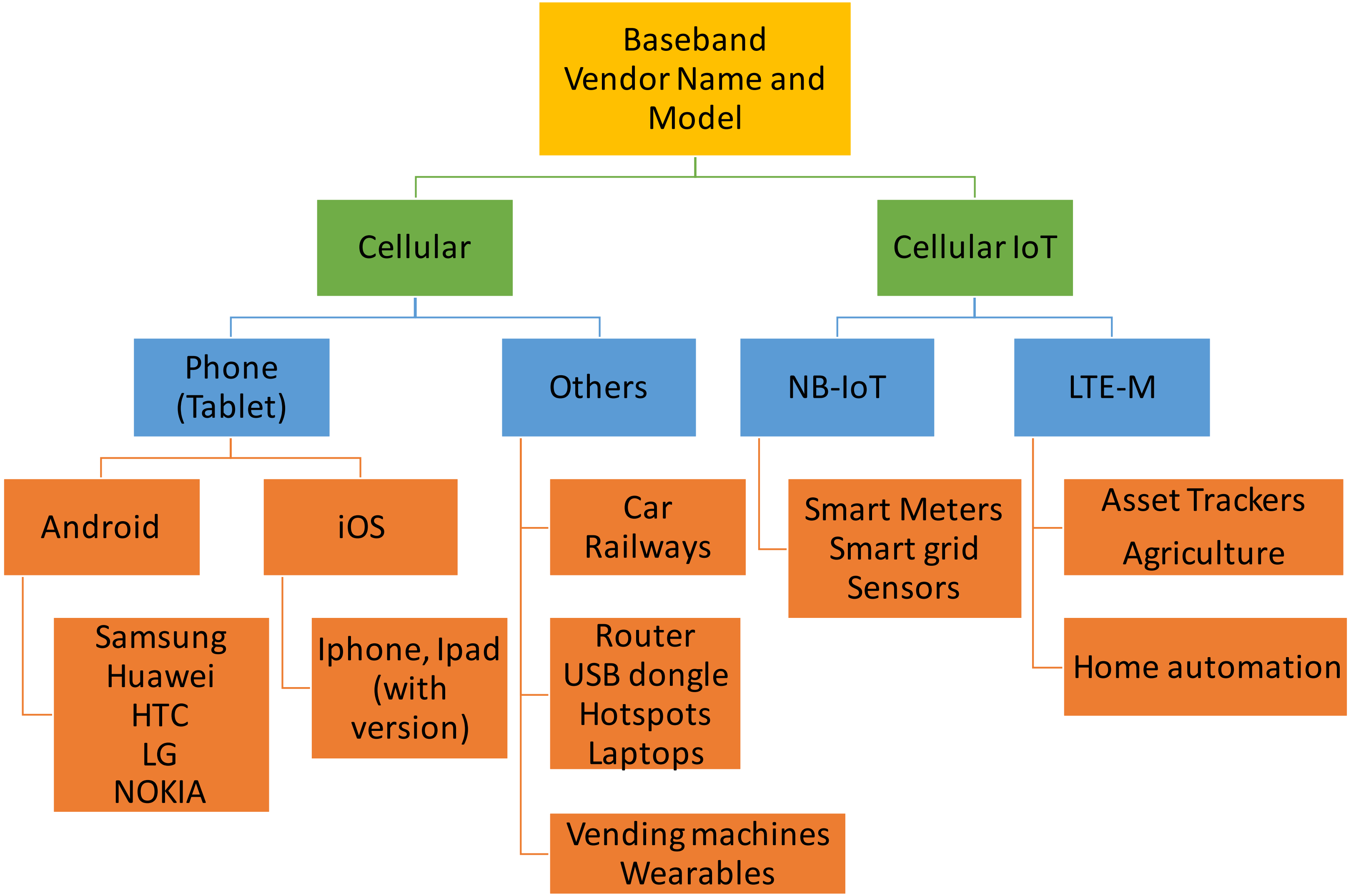


```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp   opn    smtp    Postfix smtpd
53/tcp   open   domain  ISC Bind 9.2.1
70/tcp   closed gopher
80/tcp   open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp  closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Serv-U ftpd 4.0
25/tcp    open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http         Microsoft IIS webserver 5.0
110/tcp   open  pop3         IMail pop3d 7.15 931-1
135/tcp   open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc        Microsoft Windows RPC
5800/tcp  open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

1. MNmap

Identify any Cellular device in the wild

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


Baseband Vendor Name and Model
Cellular
Cellular IoT
Phone (Tablet)
Others
NB-IoT
LTE-M
Android
iOS
Samsung Huawei HTC LG NOKIA
Iphone, Ipad (with version)
Car Railways
Router USB dongle Hotspots Laptops
Vending machines Wearables
Smart Meters Smart grid Sensors
Asset Trackers Agriculture
Home automation

Identification – How

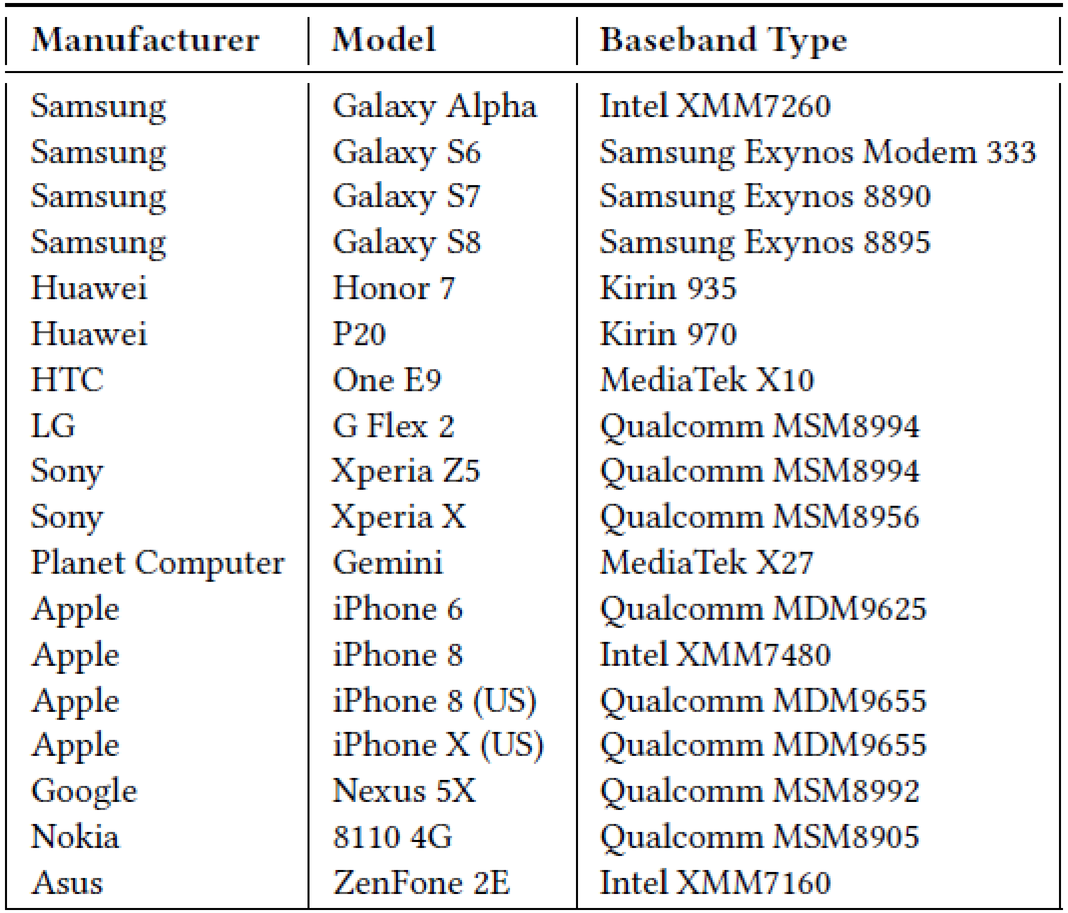
Baseband Vendors implement capabilities differently

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

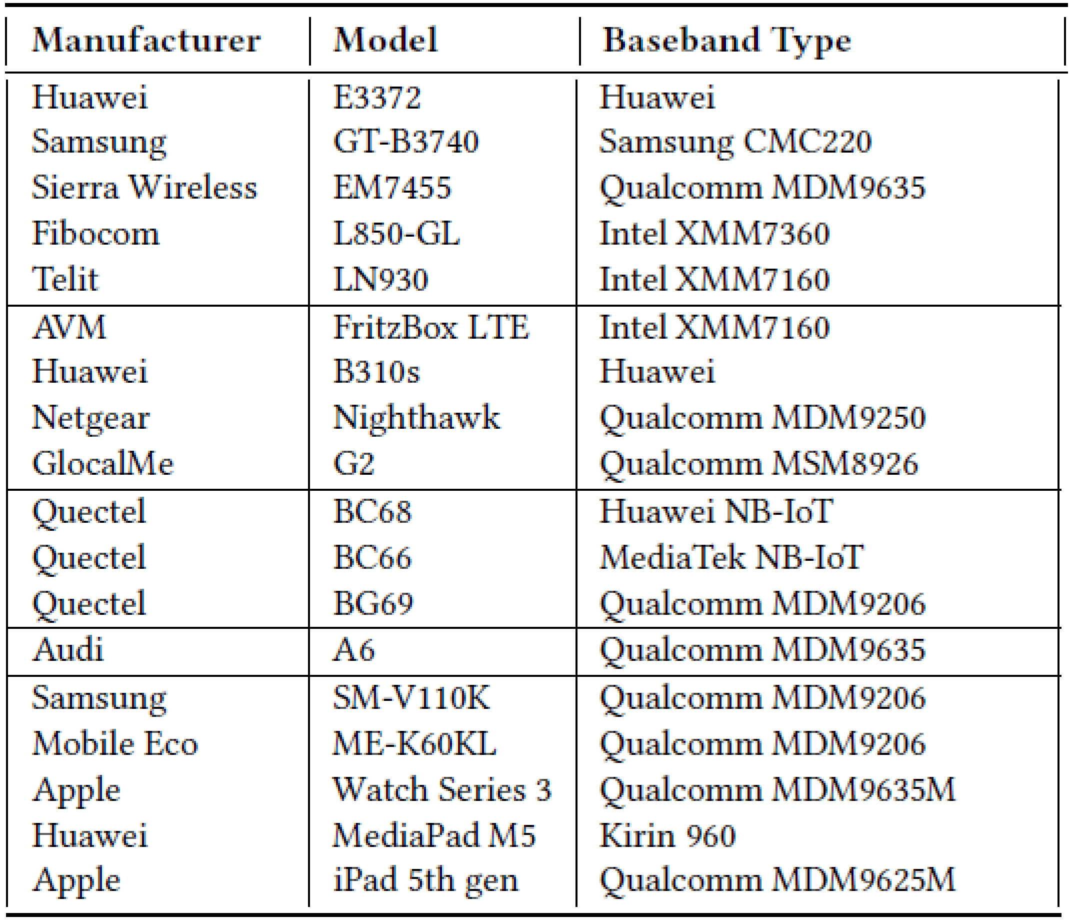
Each target Application requires different set of UE Capabilities

- 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)

DUT



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

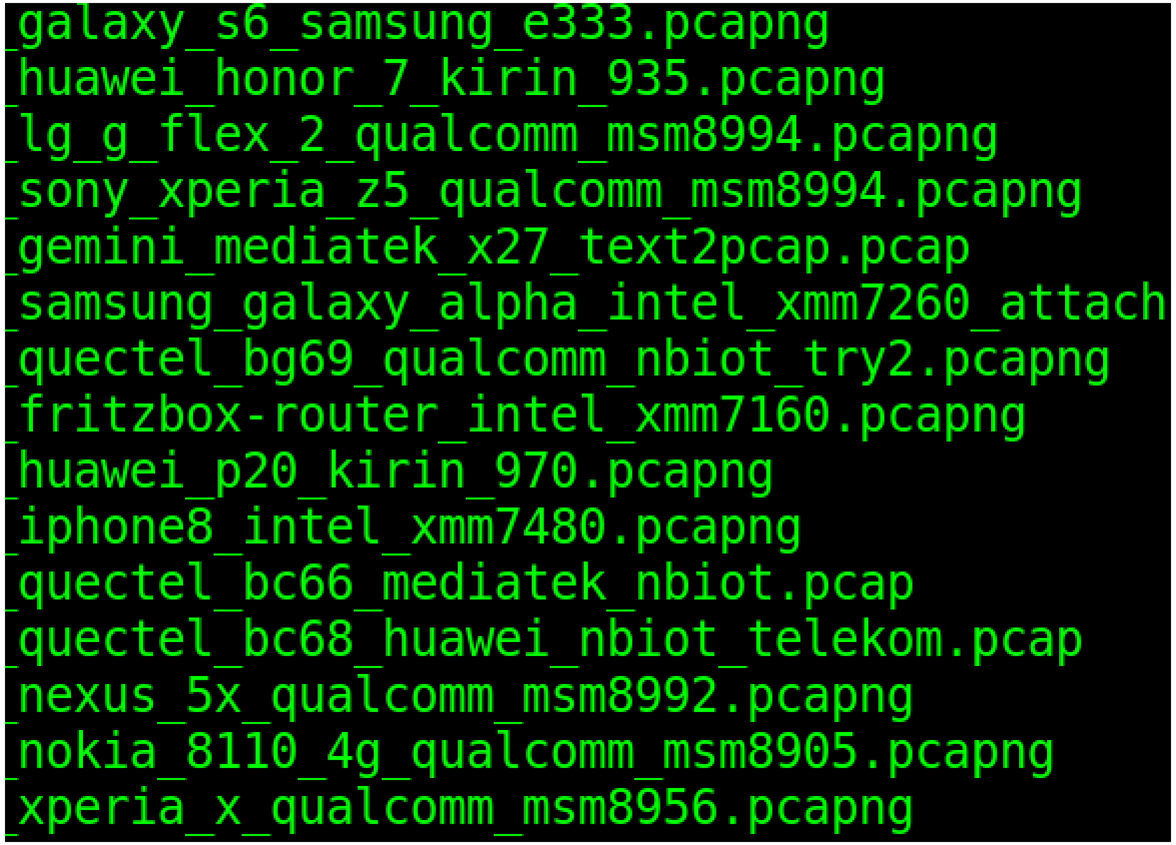


Manufacturer	Model	Baseband Type
Huawei	E3372	Huawei
Samsung	GT-B3740	Samsung CMC220
Sierra Wireless	EM7455	Qualcomm MDM9635
Fibocom	L850-GL	Intel XMM7360
Telit	LN930	Intel XMM7160
AVM	FritzBox LTE	Intel XMM7160
Huawei	B310s	Huawei
Netgear	Nighthawk	Qualcomm MDM9250
GlocalMe	G2	Qualcomm MSM8926
Quectel	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



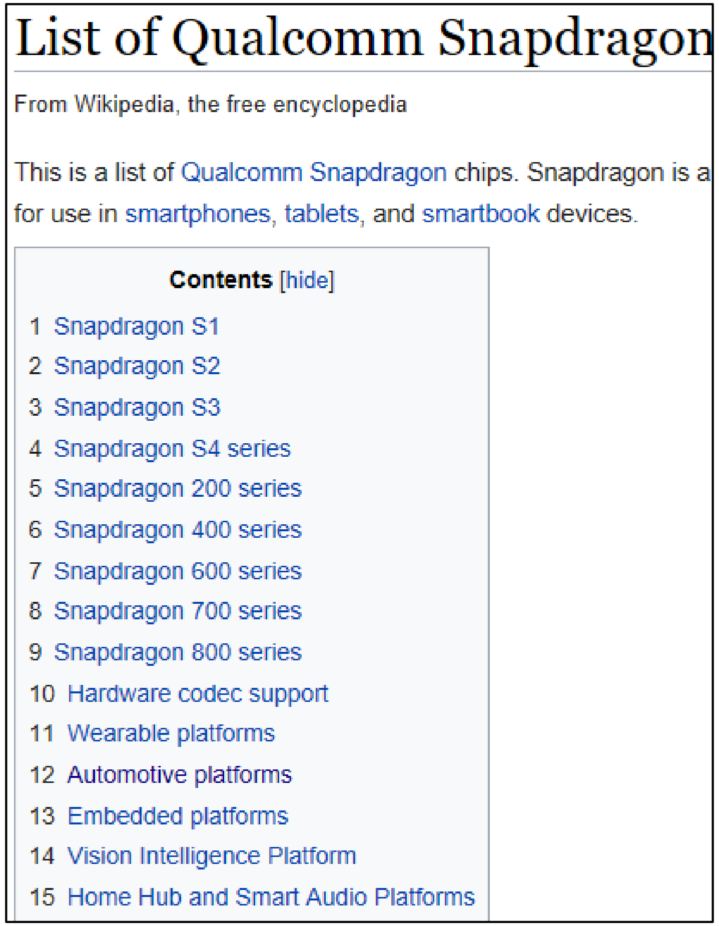
```
_galaxy_s6_samsung_e333.pcapng
_huawei_honor_7_kirin_935.pcapng
_lg_g_flex_2_qualcomm_msm8994.pcapng
_sony_xperia_z5_qualcomm_msm8994.pcapng
_gemini_mediatek_x27_text2pcap.pcap
_samsung_galaxy_alpha_intel_xmm7260_attach
_quectel_bg69_qualcomm_nbiot_try2.pcapng
_fritzbox-router_intel_xmm7160.pcapng
_huawei_p20_kirin_970.pcapng
_iphone8_intel_xmm7480.pcapng
_quectel_bc66_mediatek_nbiot.pcap
_quectel_bc68_huawei_nbiot_telekom.pcap
_nexus_5x_qualcomm_msm8992.pcapng
_nokia_8110_4g_qualcomm_msm8905.pcapng
_xperia_x_qualcomm_msm8956.pcapng
```

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

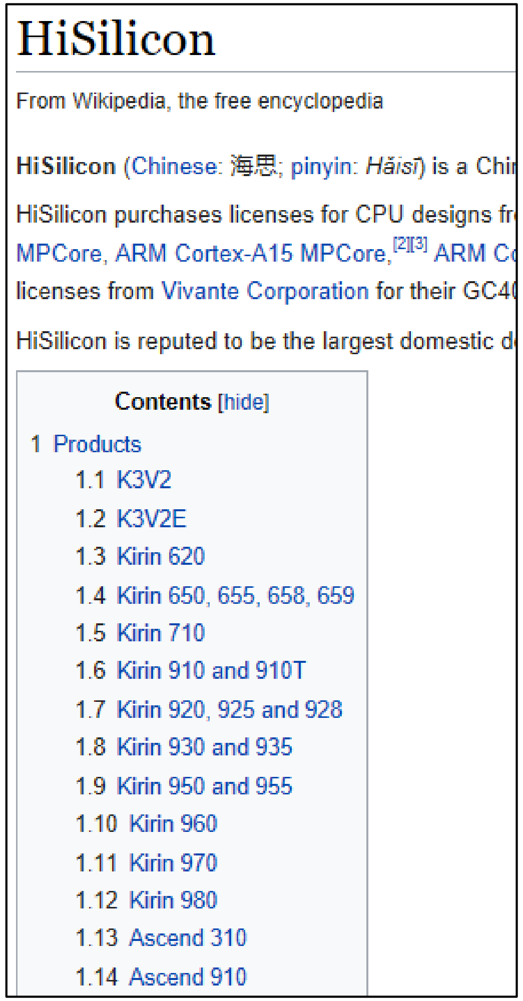


List of Qualcomm Snapdragon

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

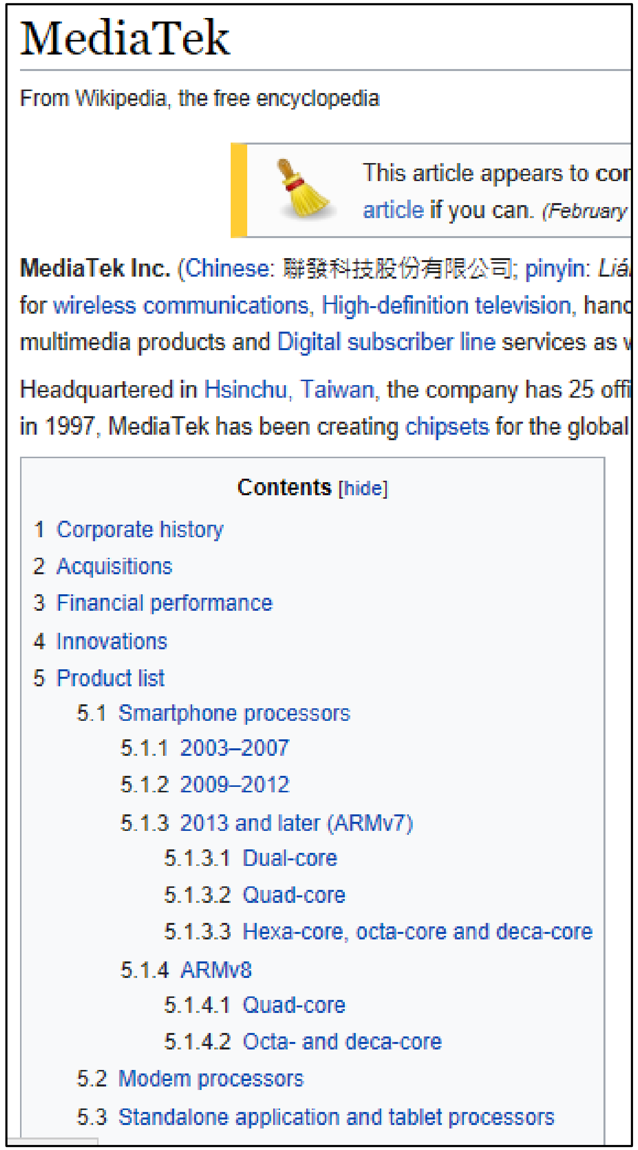
From Wikipedia, the free encyclopedia

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

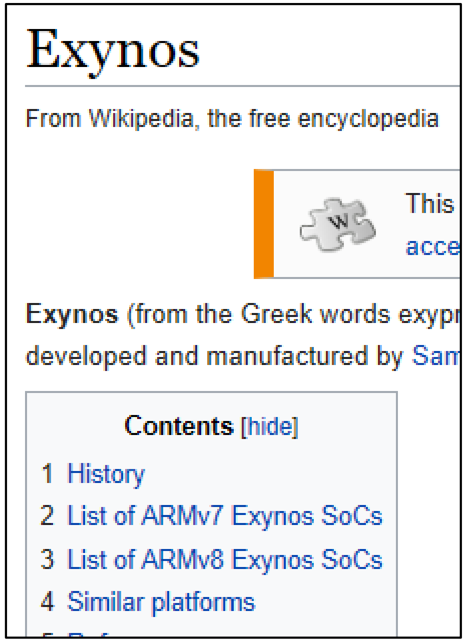
From Wikipedia, the free encyclopedia

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

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

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 exypr
developed and manufactured by Sam

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

Difference b/w iOS and Android

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

Phone and preferred Baseband

Phone	Baseband
Huawei	Huawei
Samsung	Samsung
Apple	Intel or QCT

Difference b/w cellular and cellular IoT

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

MNmap issues

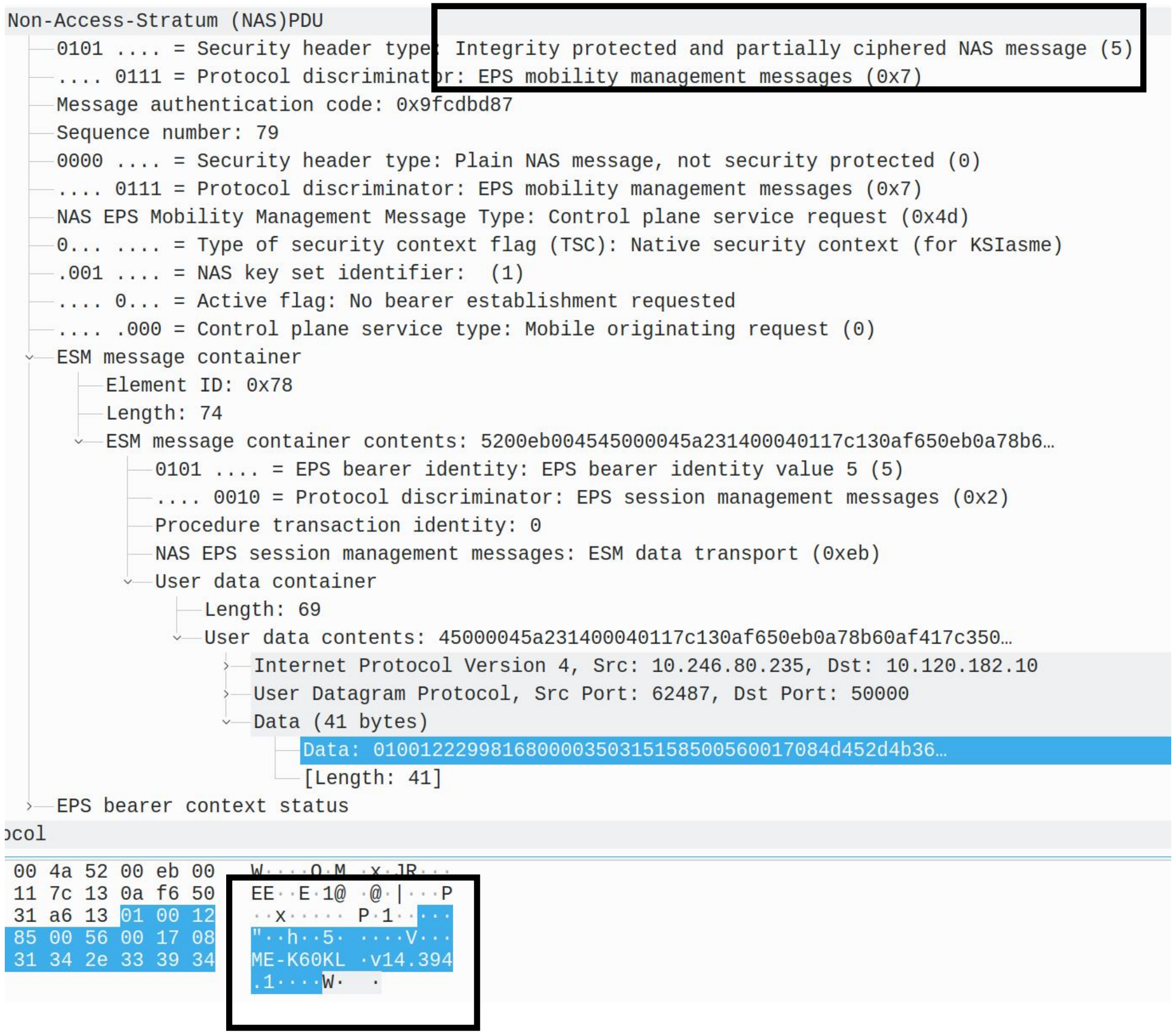
- SIM card can have affect on capabilities
  - enabled/disabled – operator setting, e.g., bands

- 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**



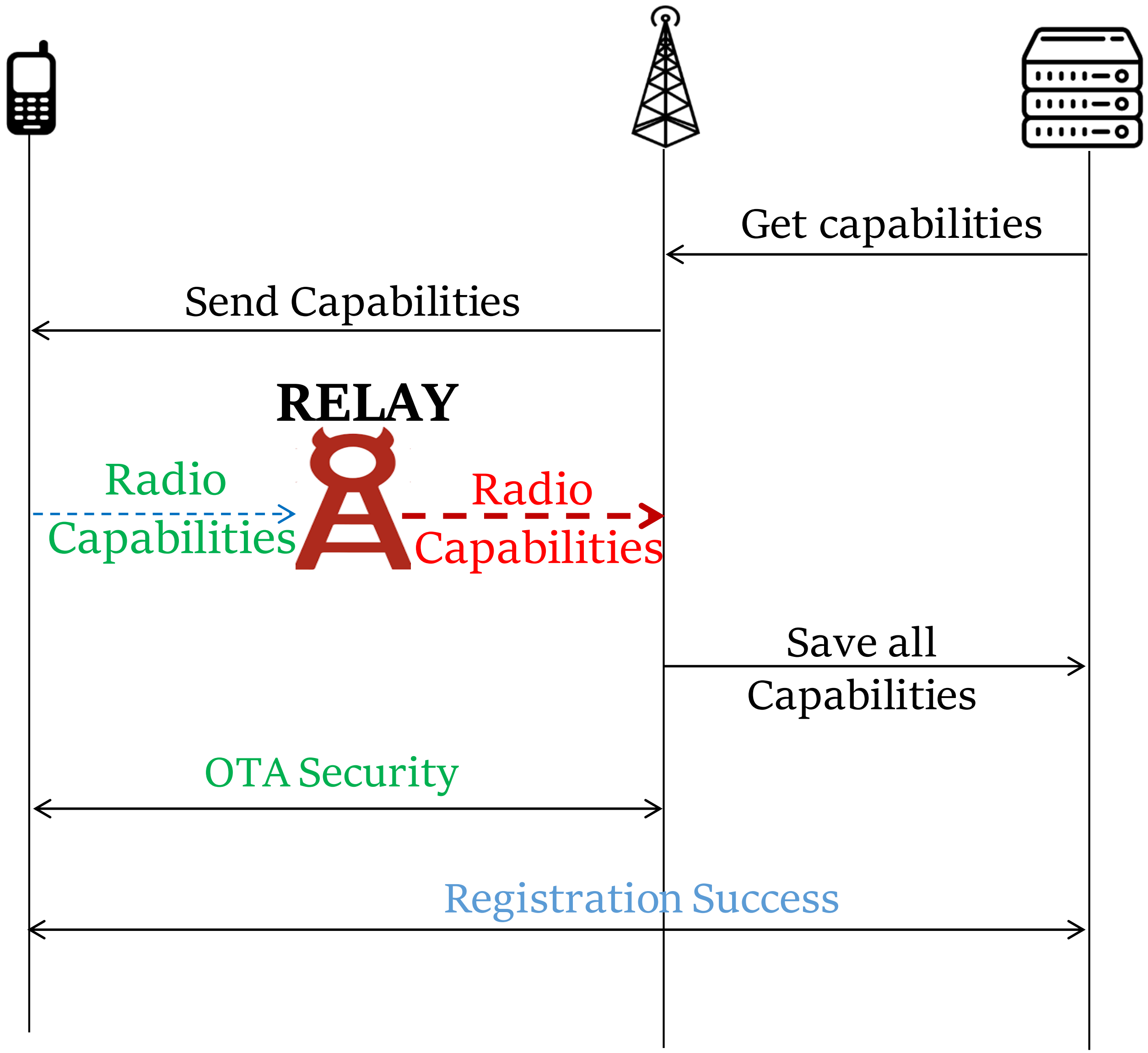
```
Non-Access-Stratum (NAS)PDU
    0101 .... = Security header type: Integrity protected and partially ciphered NAS message (5)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
    Message authentication code: 0x9fcdbd87
    Sequence number: 79
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
    NAS EPS Mobility Management Message Type: Control plane service request (0x4d)
    0... .... = Type of security context flag (TSC): Native security context (for KSIasme)
    .001 .... = NAS key set identifier:  (1)
    .... 0... = Active flag: No bearer establishment requested
    .... .000 = Control plane service type: Mobile originating request (0)
  ⌄ ESM message container
        Element ID: 0x78
        Length: 74
      ⌄ ESM message container contents: 5200eb004545000045a231400040117c130af650eb0a78b6…
            0101 .... = EPS bearer identity: EPS bearer identity value 5 (5)
            .... 0010 = Protocol discriminator: EPS session management messages (0x2)
            Procedure transaction identity: 0
            NAS EPS session management messages: ESM data transport (0xeb)
          ⌄ User data container
                Length: 69
              ⌄ User data contents: 45000045a231400040117c130af650eb0a78b60af417c350…
                  › Internet Protocol Version 4, Src: 10.246.80.235, Dst: 10.120.182.10
                  › User Datagram Protocol, Src Port: 62487, Dst Port: 50000
                  ⌄ Data (41 bytes)
                        Data: 0100122299816800003503151585005600170840d452d4b36…
                        [Length: 41]
  › EPS bearer context status
ocol

 00 4a 52 00 eb 00     W····O·M ·x·JR···
 11 7c 13 0a f6 50     EE··E·1@ ·@·|···P
 31 a6 13 01 00 12     ··x·····  P·1····
 85 00 56 00 17 08     "··h··5· ····V···
 31 34 2e 33 39 34     ME-K60KL ·v14.394
                       .1····W·  ·
```

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 with interested researchers

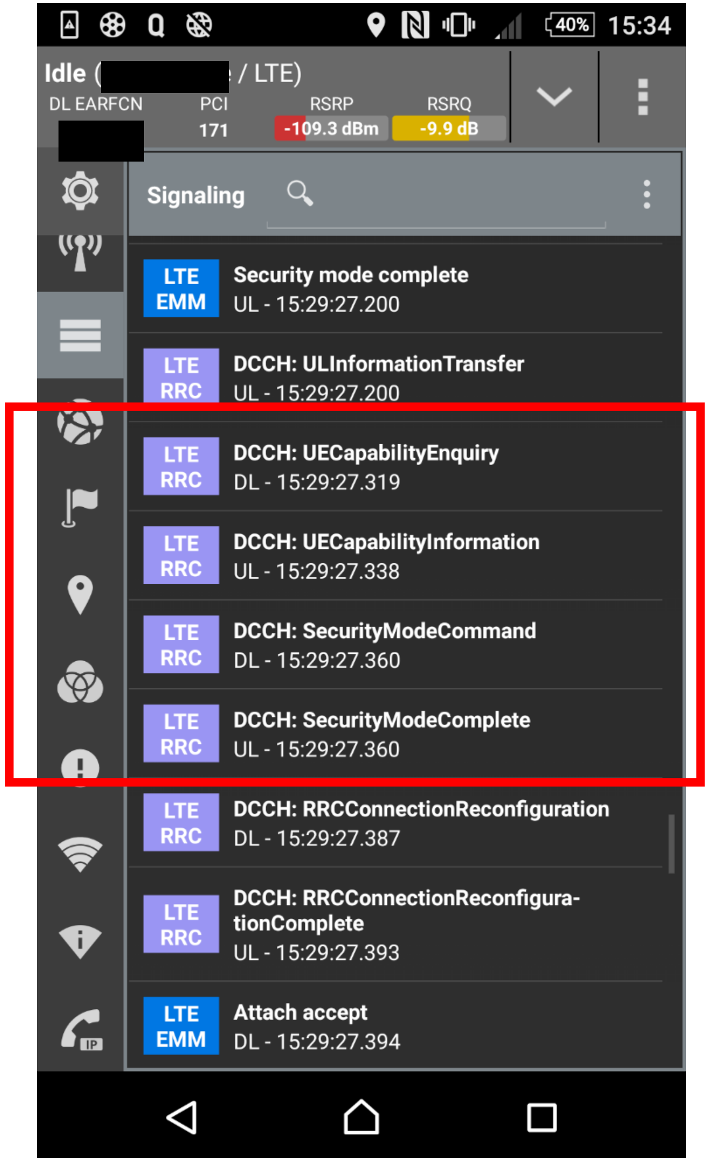
2. Bidding down

- Hijacking
    - Radio Capabilities
    - MitM relay before OTA Security
    - Network 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



40% 15:34

Idle ([redacted] / LTE)

DL EARFCN	PCI	RSRP	RSRQ
[redacted]	171	-109.3 dBm	-9.9 dB

Signaling

LTE EMM	Security mode complete UL - 15:29:27.200
LTE RRC	DCCH: ULInformationTransfer UL - 15:29:27.200
LTE RRC	DCCH: UECapabilityEnquiry DL - 15:29:27.319
LTE RRC	DCCH: UECapabilityInformation UL - 15:29:27.338
LTE RRC	DCCH: SecurityModeCommand DL - 15:29:27.360
LTE RRC	DCCH: SecurityModeComplete UL - 15:29:27.360
LTE RRC	DCCH: RRCConnectionReconfiguration DL - 15:29:27.387
LTE RRC	DCCH: RRCConnectionReconfigurationComplete UL - 15:29:27.393
LTE EMM	Attach accept DL - 15:29:27.394

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

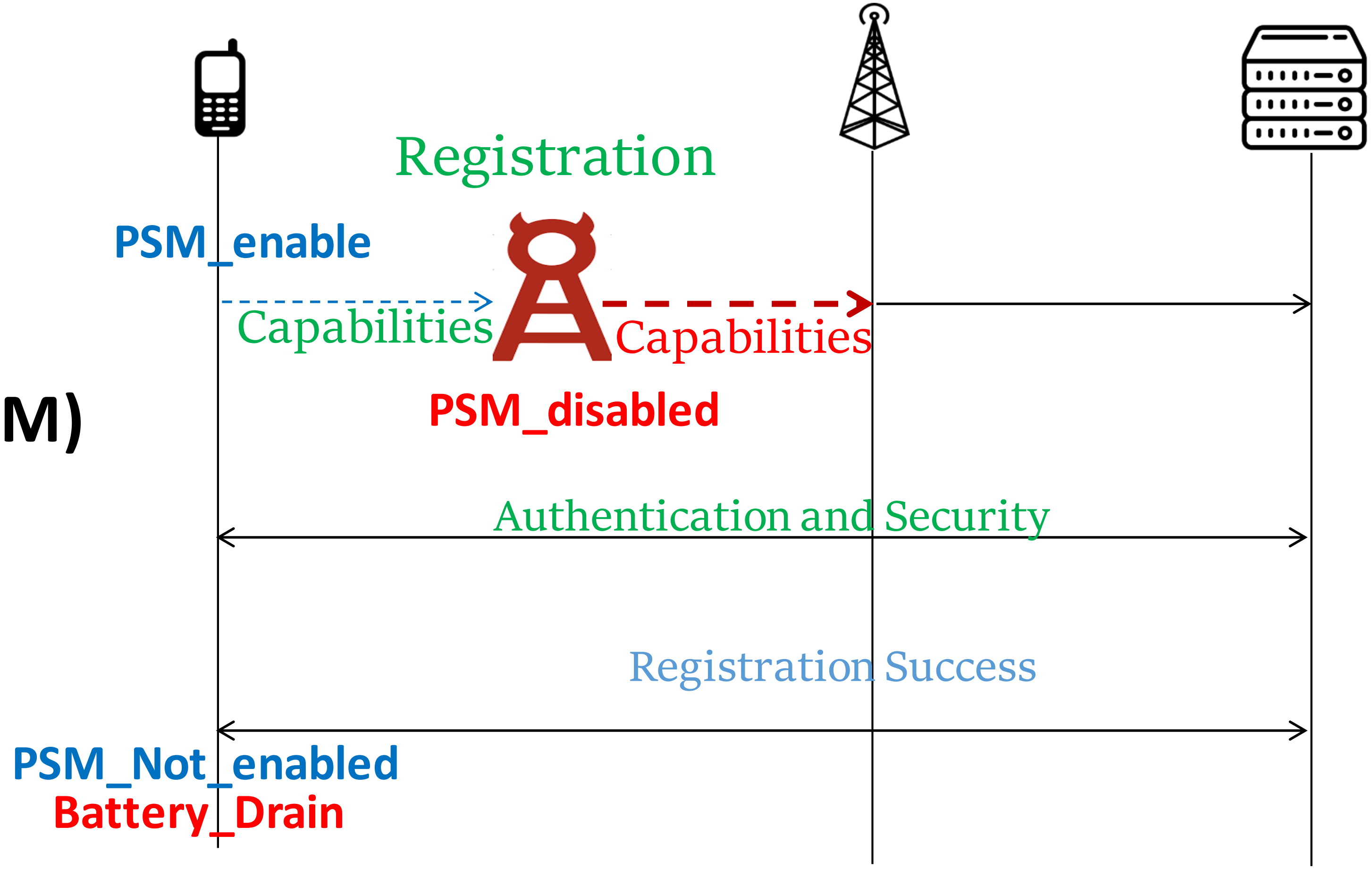
- **22 out of 32** Tested LTE networks worldwide (Europe, Asia, NA) are affected (USA, Switzerland, France, Japan, Korea Netherlands, UK, Belgium, Iceland)

- Persistent for 7 days
  - Capabilities are Cached at Core network
  - Restart device for normal operation

- **Radio is bottleneck for speed data service

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**

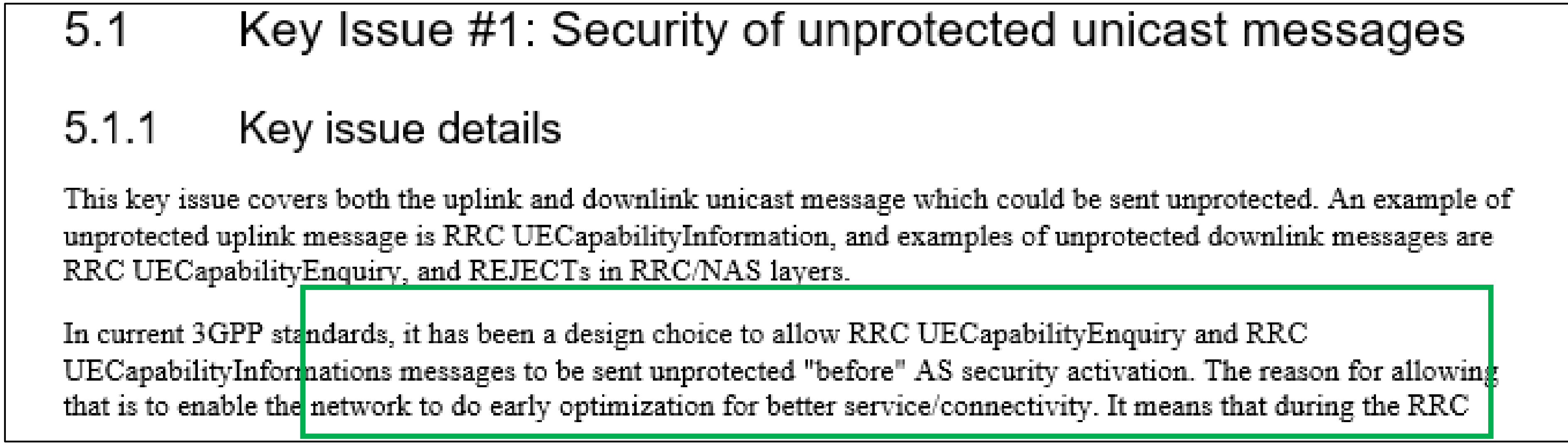
- Persistent attack: restart required to restore

Vulnerability Status

- Reported to GSMA, 3GPP SA3 and other affected operators and vendors
- Positive acknowledgement / could be implementation issues
- GSMA sent a LS (Liaison statement) to 3GPP to add fixes
- Core network capabilities are still unprotected
  - MNmap still possible on 5G

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

Fixes

- ✓ Fixes in LTE release 14 for NB-IoT will be commercial soon

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

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

Thank you

✉ altaf329@sect.tu-berlin.de

rbbo@kth.se