P1 Security
Priority One Security

5G UE Handsets and SoCs

C5202-p1

P1 Security Training

Table of Content (Agenda)

1. Introduction
2. 5G modem solutions and roadmaps
3. Millimetric wavelengths (mmWave)
4. Handset complexity
    a. Hardware
    b. Software
5. Recent (and older) vulnerabilities
6. Conclusion
7. Q&A and Discussion
8. Annex: some more info on UE

Introduction

Why care about 5G UE / 5G Phones?

- **Subscriber's communication and data security relies on the security of its phone**
  - Good understanding of the phone security, including baseband, is important
- **Phone firmware analysis often show what will future network offer as services**
  - First batch of terminals for a new technology often has
    - extended debugging capabilities (debugging symbols…)
    - hardware debugging interface unlocked
    - implementation issues regarding certain security features (both at cellular and system level)
- **Good sources of Android firmware / ROM:**
  - https://forum.xda-developers.com/

5G modem solutions and roadmaps

5G UE Availability

Back in May 2019, following initial commercial deployments and service availability

Vendor	Region
Samsung	South Korea
Huawei HiSilicon	Switzerland UK (June TBC)
Qualcomm	US (Verizon) Switzerland UK

Since then, new 5G networks have been open to customers in Belgium, Netherland, Poland, Finland, Sweden, Canada, France…

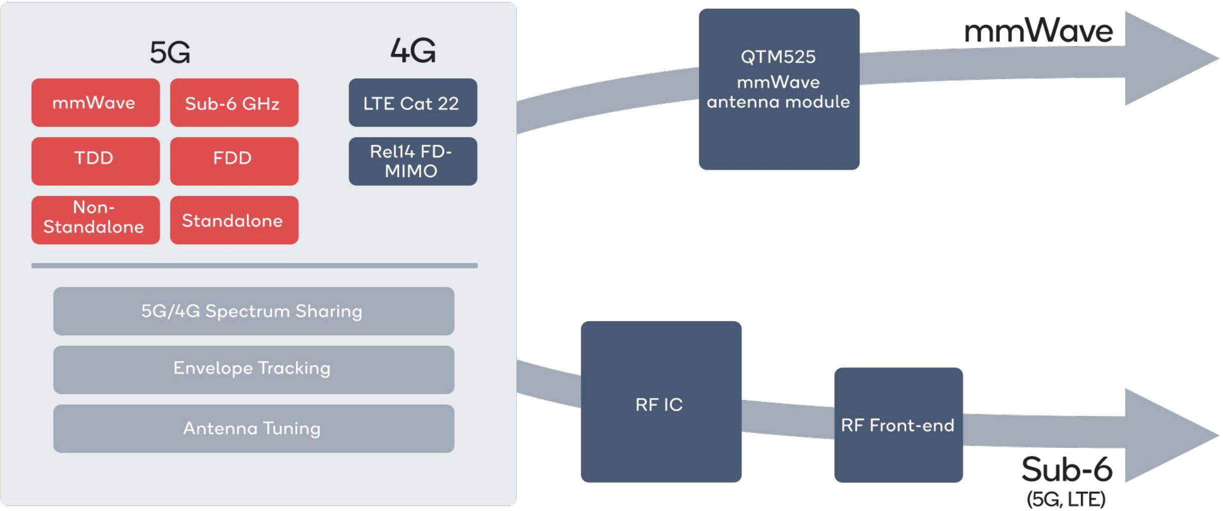
See for example:
https://www.speedtest.net/ookla-5g-map

Moreover, Mediatek entered the 5G SoC market in 2021 while Unisoc-based 5G devices may appear in late 2022.

Qualcomm modem solutions

- **2 modems initially proposed in 2019:**
    - X50 (SDX50), standalone 5G modem, with support for sub-6GHz and mmWave frequencies, TDD mode and NSA architecture only
    - X55, integrated multi-RAT modem (2G to 5G), 5G with additional support for FDD mode and SA architecture, LTE Rel.14 ; baseband integrated within SnapDragon SoC

"We expect our 5G platform to [...] power virtually all 5G launches in 2019 […]" said Cristiano Amon, president, Qualcomm Incorporated
Image source: https://www.qualcomm.com/products/snapdragon-x55-5g-modem



Qualcomm RF Front-End modules

- **Starting in 2019, Qualcomm extended greatly its RF product-line:**
  - Power amplifiers QPM56XY and QPM58XY, to support all 4G / 5G, UL (PA) / DL (LNA) combinations
  - Envelope tracker QET6100, to support 5G NR specificities
  - 5G sub-6GHz adaptive antenna tuning solution QAT3555
  - 5G mmWave antenna dedicated modules QTM052 and QTM525
    - QTM535 and QTM545 available in 2022

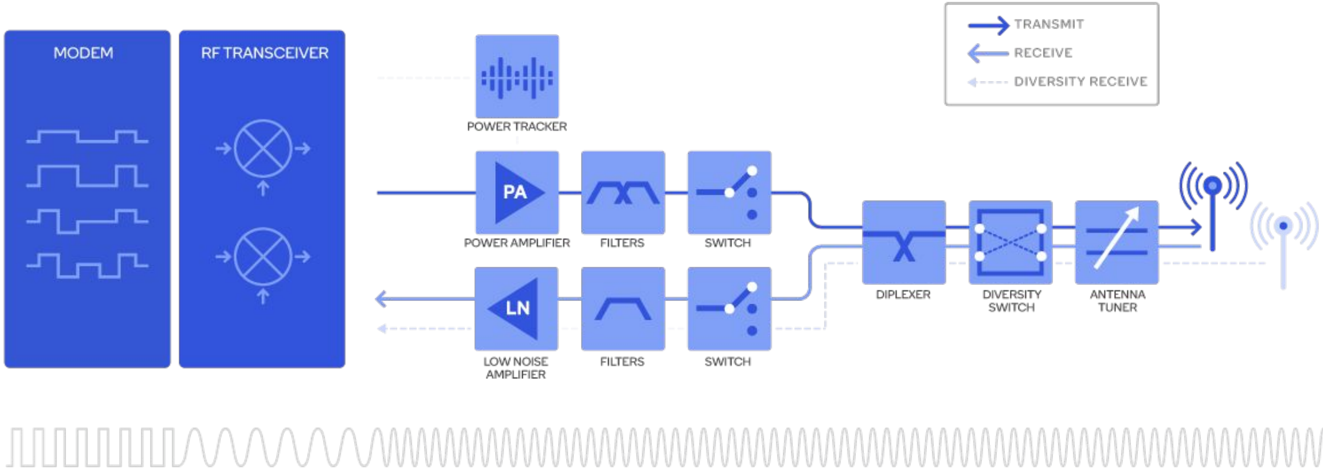


Image source: https://www.qualcomm.com/products/rf

Qualcomm latest modem solutions

- **In 2020:**
  - X60 (SDX60), standalone 5G modem, with support for sub-6GHz and mmWave frequencies, TDD / FDD modes and NSA / SA
  - 5G mmWave - sub-6 aggregation, sub-6 carrier aggregation across FDD and TDD
    - 5G mmWave: 800 MHz bandwidth, 8 carriers, 2x2 MIMO
    - 5G sub-6 GHz: 200 MHz bandwidth, 4x4 MIMO
    - 4G / 5G Dynamic Spectrum Sharing (DSS)
    - 5G Peak Download Speed: 7.5 Gbps, 5G Peak Upload Speed: 3 Gbps
  - Present in smartphones launched in early 2021

- **In 2021:**
  - X65: 10 gigabit 5G modem and 3GPP release 16 compliant
    - Complete set with baseband and RF components
    - https://www.qualcomm.com/products/snapdragon-x65-5g-modem-rf-system
  - Snapdragon 888 SoC (SM8350) integrates the X60 baseband
    - Xiaomi Mi11 teardown: https://www.ifixit.com/Teardown/Xiaomi+Mi+11+Teardown/141047

Handset complexity

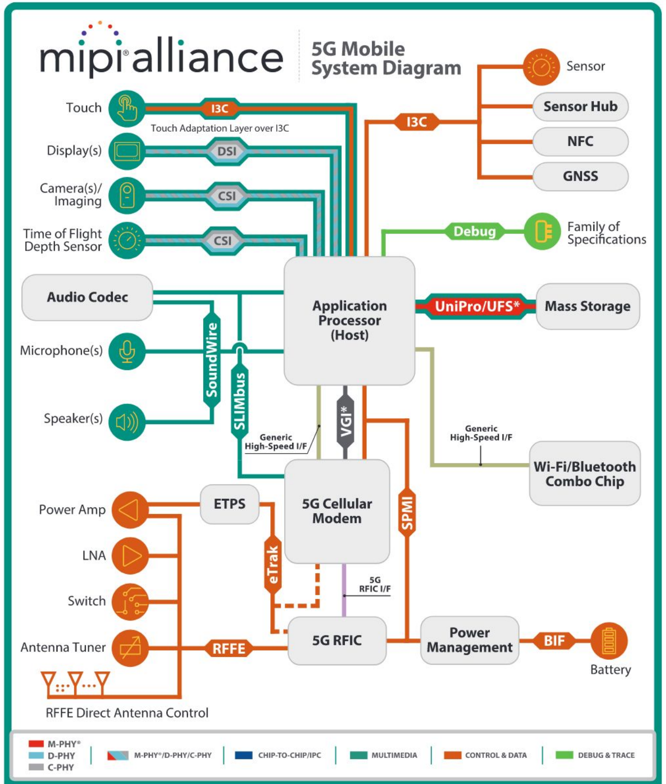
C5202-p2

P1 Security Training

Physical design

- **4G handsets achieved a very good integration**
    - Single SoC integrating multi-core Application Processor (AP), Baseband Processor (BP), and many other peripherals
    - Integrated 2G-3G-4G RF components (LNA / power amplifiers, filters, antennas)
- **New 5G multi-technologies handsets are getting more complex, physically**
    - Separate baseband processor in early designs from 2019/2020 (Qualcomm X50, Exynos 5100…)
        - Requires specific interconnect with the main processor and RAM
        - Starting in 2021/2022, 5G modems get reintegrated into the main SoC (e.g. Snapdragon 8 Gen 1, as in the Motorola Edge X30)
    - More RF components
    - More antennas (for bigger MIMO configuration)
    - Even more RF and antennas for mmWave support

5G UE hardware architecture example



*Dark grey indicates specifications still in development.

*The UFS (Universal Flash Storage) specification from JEDEC uses the MIPI M-PHY physical layer and MIPI UniPort-M.

MIPI, DigRF, M-PHY, SLIMbus, and SoundWire are registered service marks of MIPI Alliance. All other MIPI specification names are service marks of MIPI Alliance. [Third party marks are the property of their respective owners.]

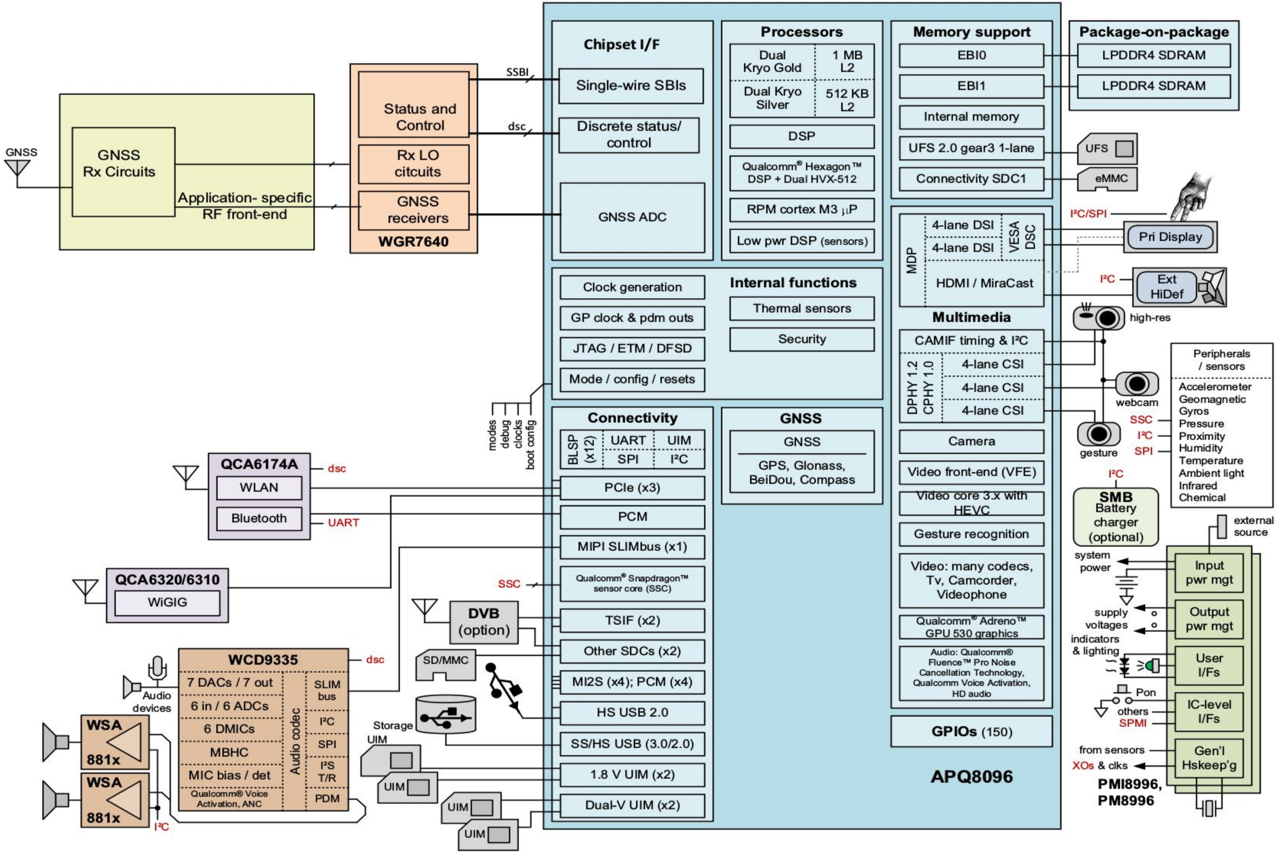
©MIPI Alliance, Inc. | September 2018

- **MIPI Alliance:**
  - develops physical / wired protocols for various embedded systems
  - audio, camera and imaging (e.g. CSI cam / DSI display)
  - chip-to-chip for inter-processor / RAM (e.g. LLI)
  - analog and digital RF (RFFE, FEM...)
  - interface to sensors, battery, power-management system, GPIO
  - PHY trace and debugging systems

Image source: https://mipi.org/5g-readiness-assessment-mipi-specifications-page-2

P1 Security
Priority One Security

Snapdragon 820e (no cellular modem)



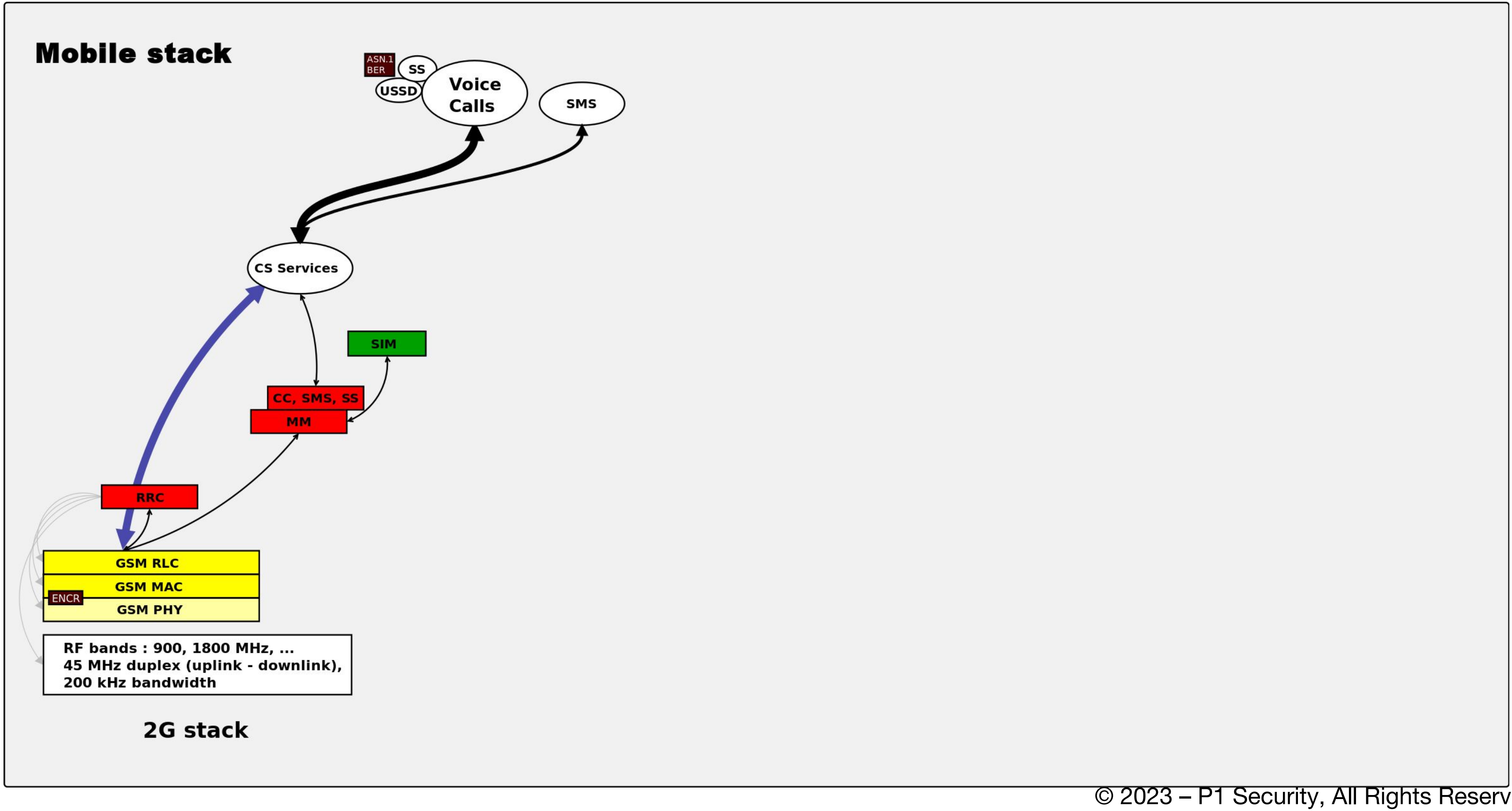
Qualcomm APQ8096SGE functional block diagram and example application

Image source: https://developer.qualcomm.com/qfile/35457/lm80-p2751-1_e.pdf

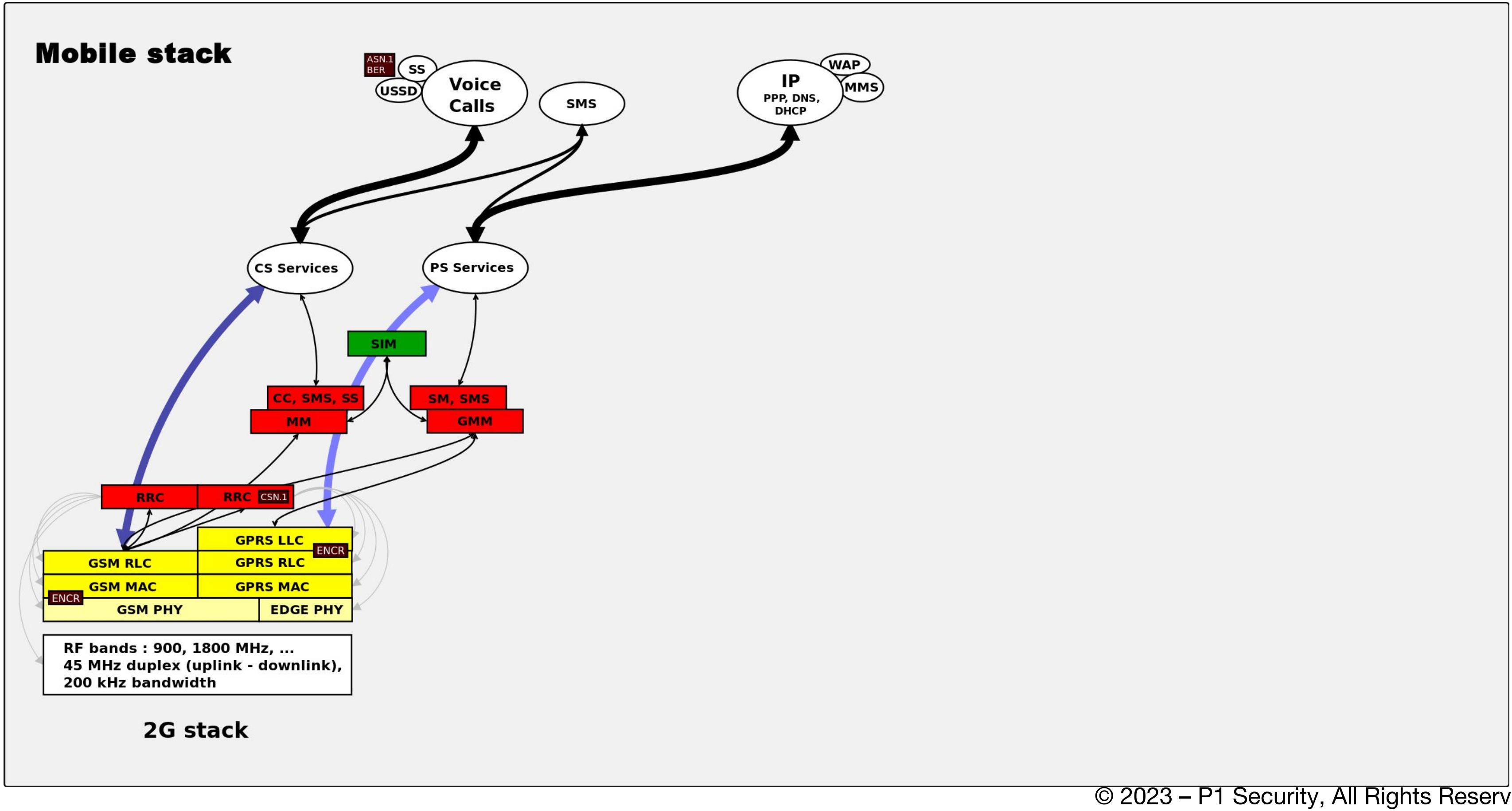
Software stack

- **Cellular radio stacks:**
  - GSM/GPRS/EDGE (2G)
  - WCDMA (3G) and HSDPA, HSUPA, HSPA+ (3G5)
  - CDMA2000 1x / EV-DO (3G, North America)
  - TD-SCDMA (3G, China)
  - LTE FDD and TDD (4G), LTE-Advanced (4G+)
  - 5GNR, FDD and TDD, NSA and SA, sub-6GHz and mmWave
- **Telecom services stacks:**
  - subscriber identification (UIM/SIM/USIM/ISIM, dual-SIM)
  - CS / PS / EPS services, RAT and mobility handling
  - voice calls, SMS, WAP, MMS
  - IMS, VoLTE (IPv4v6, TCP/UDP, SIP/SDP/RTP, TLS, IPsec, DTLS, SRTP…), RCS
  - geolocation (cellular-based -i.e. TDOA- and GNSS)
- **Local interfacing and application:**
  - AT command, data and audio transfer, NV memory, proprietary (DIAG, QMI…)
  - TFTP, FTP client, HTTP client, FOTA...

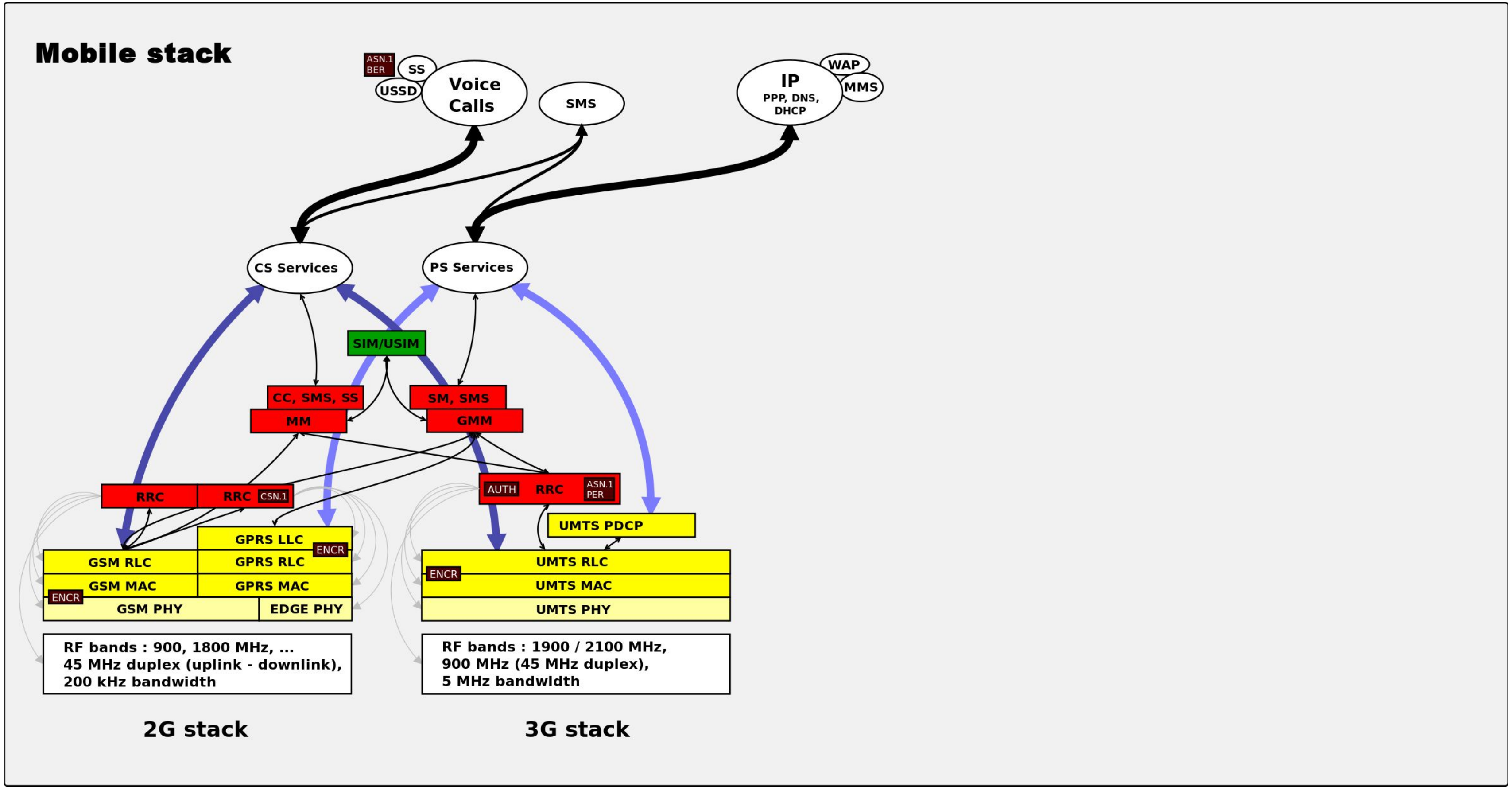
The cellular modem stack



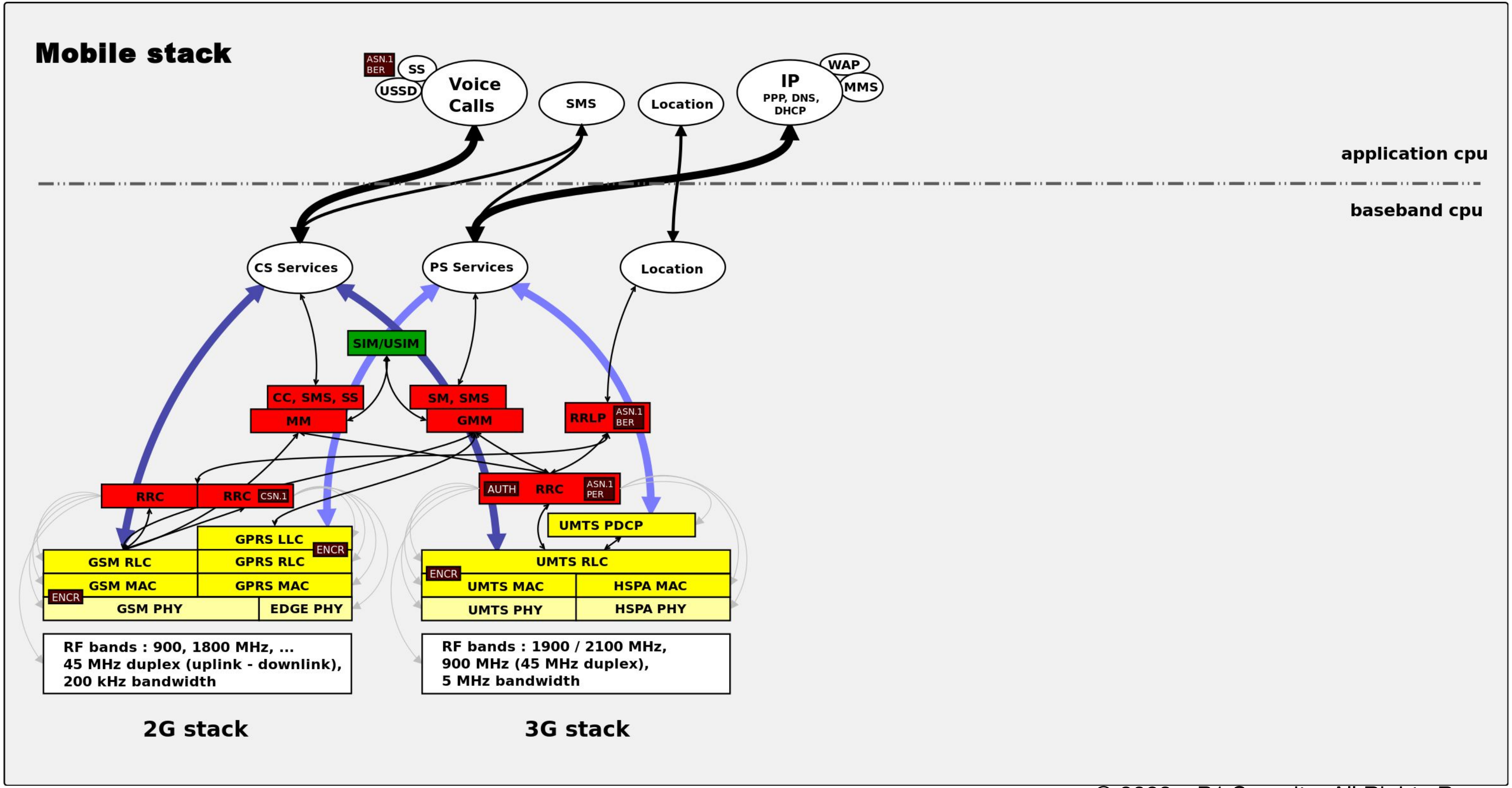
The cellular modem stack



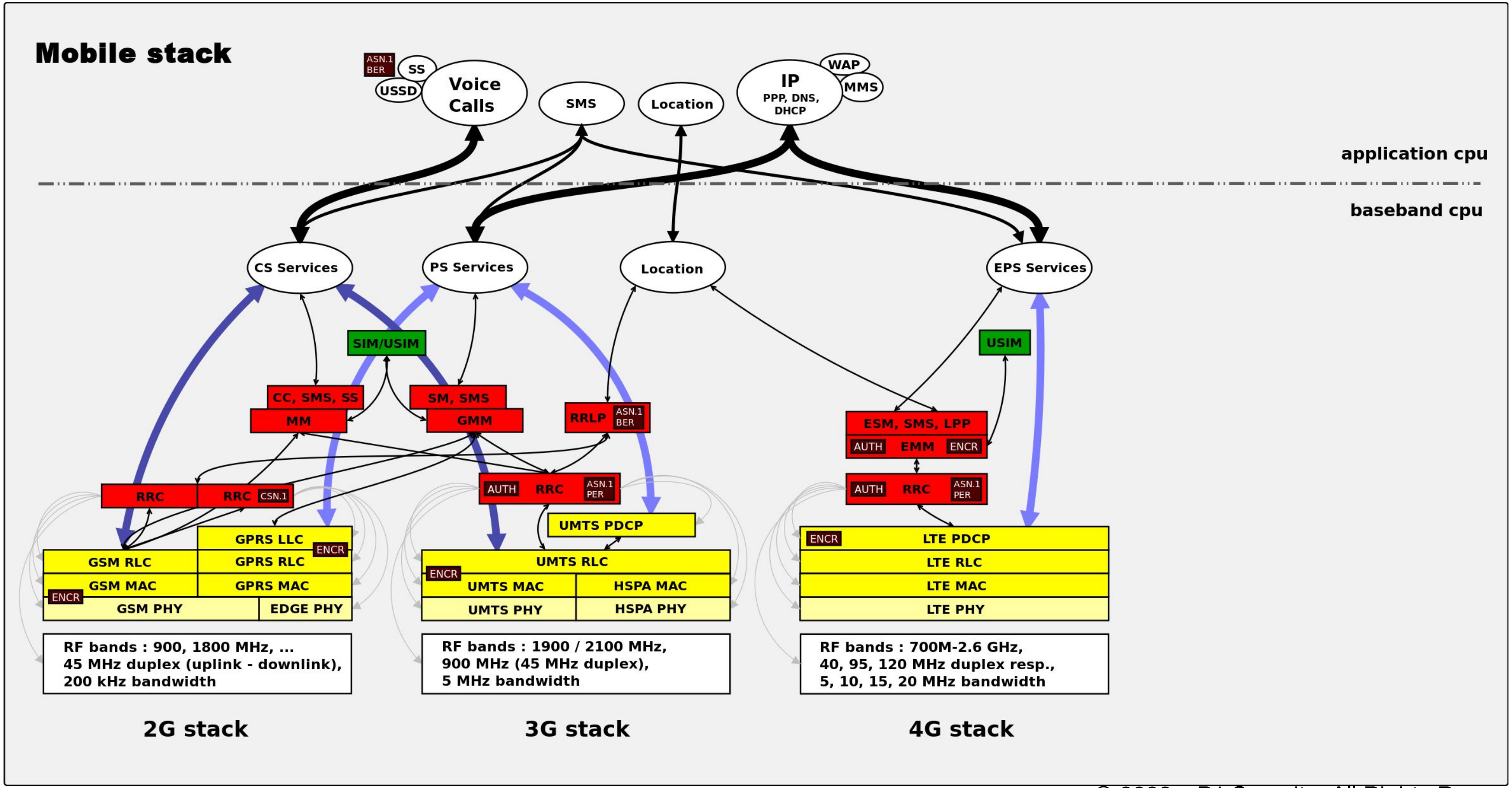
The cellular modem stack



The cellular modem stack



The cellular modem stack



RF bands : 900, 1800 MHz, ...
45 MHz duplex (uplink - downlink),
200 kHz bandwidth

RF bands : 1900 / 2100 MHz,
900 MHz (45 MHz duplex),
5 MHz bandwidth

RF bands : 700M-2.6 GHz,
40, 95, 120 MHz duplex resp.,
5, 10, 15, 20 MHz bandwidth

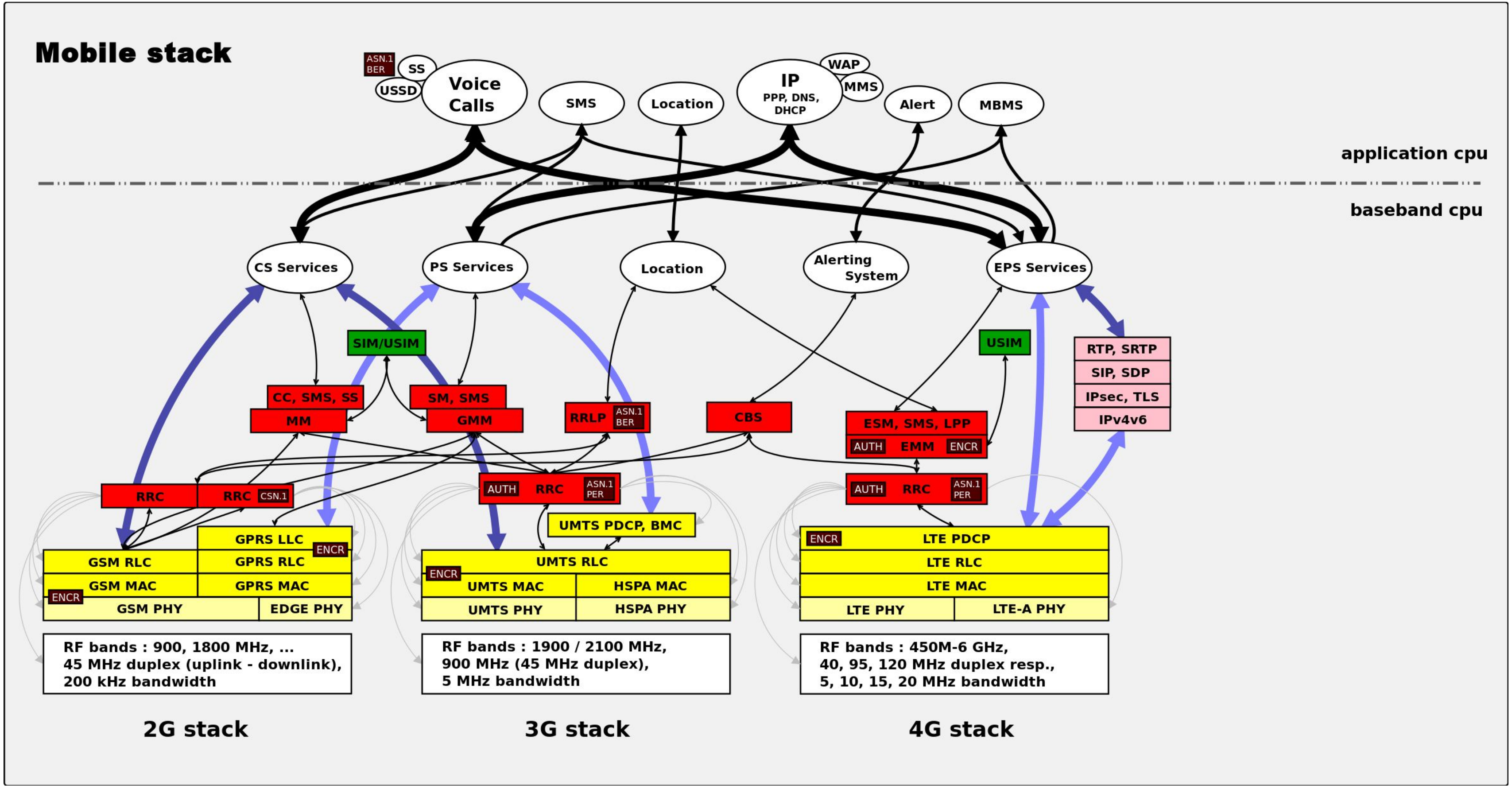
2G stack

3G stack

4G stack

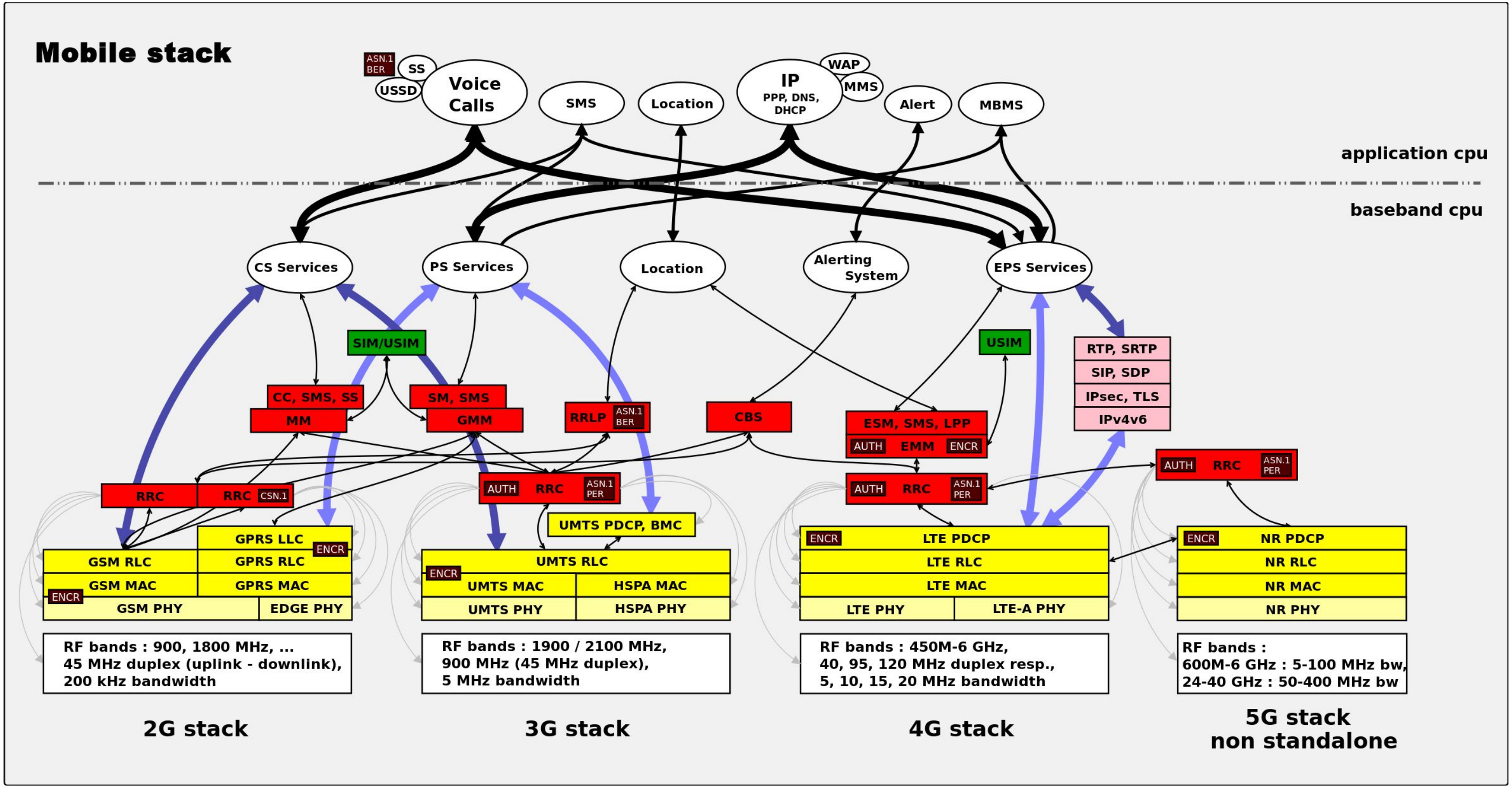
P1 Security
Priority One Security

The cellular modem stack

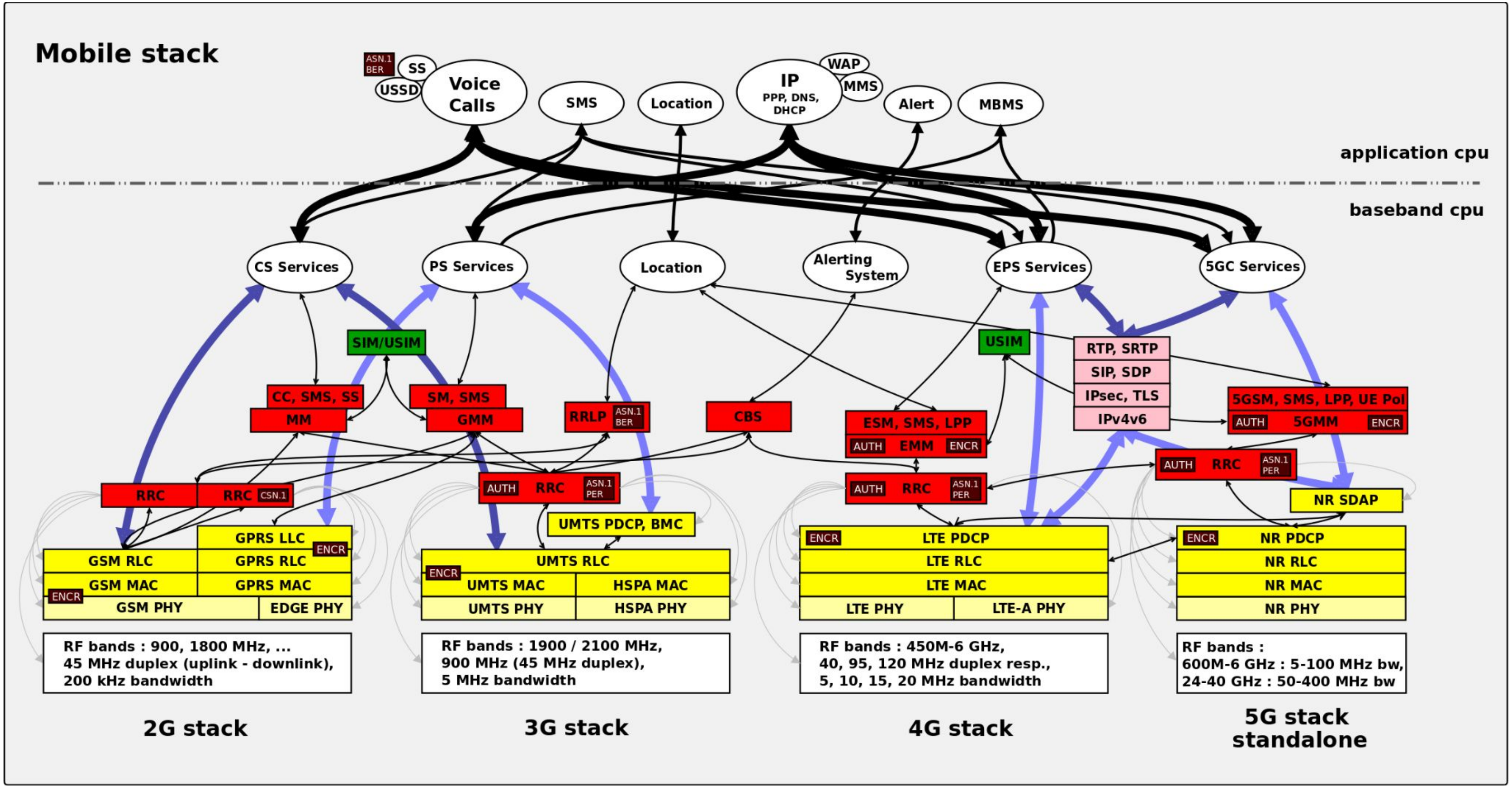


P1 Security
Priority One Security

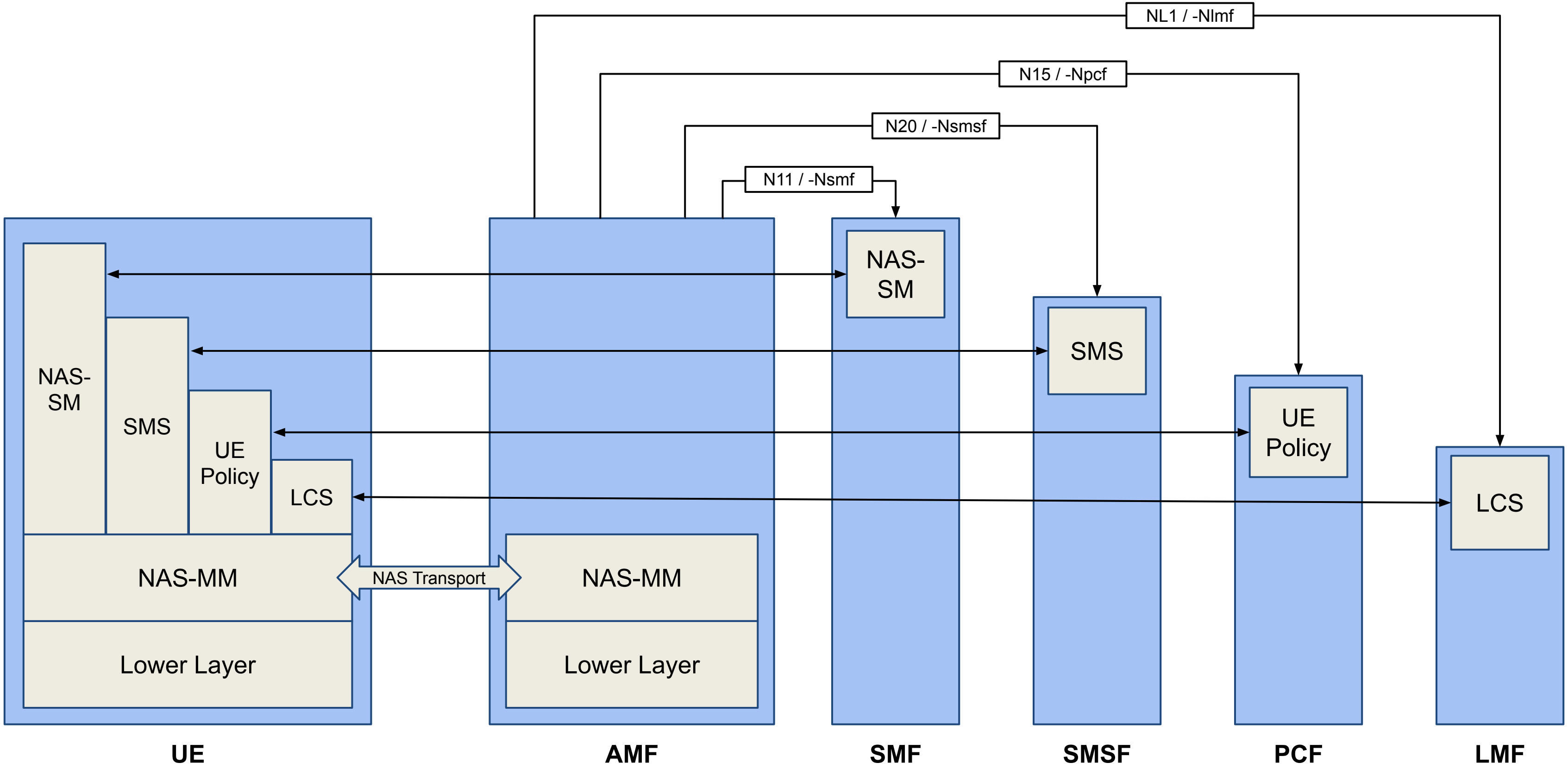
The cellular modem stack



The cellular modem stack



5G NAS protocol termination in the 5G Core



ROM analysis and binary formats

- **Not all ROMs, modems and baseband images are made equal**
  - Some easy to reverse-engineer
  - Some more difficult

Vendor & Baseband	Technology	Ease of Reverse Engineering
HiSilicon	ARM 32 bits LE, based on VxWorks 5	Easy, POSIX, debugging symbols
Qualcomm	Hexagon 32 bits LE DSP (Hexagon), based on QuRT (Qualcomm real-time kernel)	Hard, proprietary architecture, many strings but no debugging symbols
Samsung	ARM 32 bits LE , based on a Samsung proprietary runtime and executable format	Medium, ARM decompilers available, proprietary executable format, independent debugging informations

Recent (and older) vulnerabilities

C5202-p3

P1 Security Training

5G modem security overview

- **5G modem's CPU / DSP technology**
  - Software essentially written in C, some parts in C++
  - Modem executable missing standard security features:
    - system privilege separation (e.g. running in ARM supervisor mode), non-executable memory area, call-flow integrity
    - memory safety: stack cookie, "fortify" macro
  - Crypto-engine and cryptographic code not verified against state-of-the-art cache / timing / side channel and power / electromagnetic analysis
- **5G Modems are super complex**
  - Complexity => more vulnerabilities
  - Baseband vulnerability opportunity
  - Fuzzing (message's formats, state-machines transitions)
- **Unique backdooring risk**
  - Stealth backdoor, Forensics difficult, less updates
  - Always-on, reachable from kilometers away
  - Enables eavesdropping, man-in-the-middle attacks, exfiltration...

Memory-based vulnerabilities in modems

- **Initial work by RP Weinmann (2010-2012)**
  - https://comsecuris.com/papers/woot12-final24.pdf
  - stack overflow within the TMSI reallocation in iPhones (Intel baseband)
  - stack overflow through the AUTN authentication request parameter in Qualcomm basebands
  - exploit code to trigger silent calls within targeted terminals
    - diverting baseband's to execute AT auto-answer command
    - caught on a 2G fake base-station, built with OpenBTS

- **N. Golde and D. Komaromy (2015)**
  - https://comsecuris.com/blog/posts/shannon/
  - stack overflow through the "Progress Indicator" during a call setup in Samsung's baseband
  - exploit code to forward all outgoing calls to a given number

Memory-based vulnerabilities in modems

- **Comsecuris again… (2018)**
  - https://comsecuris.com/blog/posts/theres_life_in_the_old_dog_yet_tearing_new_holes_into_inteliphone_cellular_modems/
  - found several overflow in the Intel’s modem code processing broadcasted alert messages
- **Keen Security Lab of Tencent (2021)**
  - https://keenlab.tencent.com/zh/whitepapers/us-21-Over-The-Air-Baseband-Exploit-Gaining-Remote-Code-Execution-on-5G-Smartphones-wp.pdf
  - stack overflow in the IMS handler dealing with XML content of SIP bodies

Logic-based vulnerabilities in modems

- **Security bypasses (not memory-management related)**
  - SSTIC 2014: EIA0 support in Qualcomm modems
    - https://www.sstic.org/2014/presentation/Analyse_securite_modems_mobiles/ (french)
  - BlackHat 2015: modems sending UE measurement reports (containing last locations) before security activation
    - https://www.blackhat.com/eu-15/briefings.html#lte-and-imsi-catcher-myths
  - SSTIC 2016: more on various EIA0 and security activation bypasses in different modems
    - https://www.sstic.org/2016/presentation/how_to_not_break_lte_crypto/
  - “Breaking LTE on layer 2” (2019): hijacking DNS requests / responses because of the malleability of User-Plane encryption over-the-air
    - https://alter-attack.net/
  - “Dynamic security analysis of the LTE control-plane” (2019): more on various security activation bypasses in modems and network equipments
    - https://syssec.kaist.ac.kr/pub/2019/kim_sp_2019.pdf
  - “Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G” (2023): security protection bypasses in 5G modems
    - https://radix-security.com/files/2021_downgrade.pdf

Vulnerabilities in modems (pwn2own)

- **In 2017:**
  - iPhone WiFi chip
    - exploiting a chain of 4 bugs to elevate from WiFi connection to iPhone OS kernel with persistence
    - triggered just by connecting to a WiFi access point
    - https://www.thezdi.com/blog/2017/11/1/the-results-mobile-pwn2own-day-one ; see also https://googleprojectzero.blogspot.com/2017/09/over-air-vol-2-pt-1-exploiting-wi-fi.html
  - Stack overflow in HiSilicon modem
    - exploit code that rewrites the IMEI

Vulnerabilities in modems (pwn2own)

- **In 2018:**
  - Heap-overflow in the Samsung Galaxy S9 Exynos modem
    - https://www.zerodayinitiative.com/blog/2018/11/13/pwn2own-tokyo-2018-day-one-results ; see also https://www.youtube.com/watch?v=6bpxrfB9ioo
    - stack overflow through the Protocol Configuration Options IE sent during the PDP context activation procedure
    - exploit code that writes a file on the file-system
  - Failed exploit attempt against iPhoneX Intel modem
    - https://www.zerodayinitiative.com/blog/2018/11/14/pwn2own-tokyo-2018-day-two-results-and-master-of-pwn

Vulnerabilities in SMS and MMS handlers

- **Regular studies on SMS, MMS and WAP-based vulnerabilities**
  - 2009: fuzzing the iPhone SMS's handler
    - https://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-SLIDES.pdf
  - 2009: many vulnerabilities in SMS and MMS handlers
    - https://www.blackhat.com/presentations/bh-usa-09/LACKEY/BHUSA09-Lackey-AttackingSMS-SLIDES.pdf
  - 2013: rooting SIM cards through binary SMS
    - https://media.blackhat.com/us-13/us-13-Nohl-Rooting-SIM-cards-Slides.pdf
  - 2015: vulnerabilities exploited to get code execution and elevate privileges on Android terminals through the multimedia library
    - https://www.blackhat.com/docs/us-15/materials/us-15-Drake-Stagefright-Scary-Code-In-The-Heart-Of-Android.pdf
    - triggered by just receiving MMS
    - lots of work done by Google on the security of multimedia processing in Android

Vulnerabilities in OMA-DM clients

- **Work presented at Blackhat 2014**
  - https://www.blackhat.com/docs/us-14/materials/us-14-Solnik-Cellular-Exploitation-On-A-Global-Scale-The-Rise-And-Fall-Of-The-Control-Protocol.pdf
- **OMA-DM security issues enabling the bypass of the access-control and the injection of commands into terminals**
  - OMA-DM client mostly implemented in the applicative OS (Android, iPhone OS)
  - some pre-processing of messages within the modem, then forwarded to the application environment
  - OMA-DM version 1.2.1, client provided by RedBend (acquired by Harman in early 2015)
  - hardcoded symmetric key for establishing the TLS communication between the client and the server
  - impacting several US operators
- **OMA-CP still implemented by some manufacturers**
  - Older than OMA-DM, OMA-CP has no or poor authentication methods
  - https://research.checkpoint.com/advanced-sms-phishing-attacks-against-modern-android-based-smartphones/

Many vulnerabilities still to be found...

- **Cellular modems get more and more complex**
  - GSM, GPRS, EDGE, CDMA, HRPD, UMTS FDD and TDD, HSPA, LTE, LTE-A
  - ...and now 5G
  - geolocation, dual-SIM, embedded-SIM, messaging and remote management, alerting system, multimedia multicast, WiFi-interworking, proximity services, battery-saving optimizations…

- **Qualcomm almost-monopoly**
  - Samsung, Intel and HiSilicon still existing in specific products

- **Together with hardware evolution and optimization**
  - chips’ interconnections (e.g. PCIe with DMA)
  - large shared memory-mapped between the modem and the main processor
  - complex software to abstract the different types of physical interconnection

Conclusion

C5202-p4

P1 Security Training

Conclusion

- **Strong 5G Modem vendor competition at play:**
  - Qualcomm getting already a large market share for smartphones
  - Samsung and HiSilicon also available, but limited to their own smartphones
  - Mediatek appeared in low-end 5G smartphones end of 2020
  - Unisoc may appear in early 2023
- **Split hardware architecture (Main processor / modem processor)**
  - In early 5G handsets, not anymore since 2021/2022.
  - opportunity for reverse-engineering and hardware analysis and attacks
  - probability to get also firmware with extended debugging features (e.g. symbols)
- **Cellular modems only get more and more complex**
  - Just like cellular networks !
  - vulnerabilities due to older technologies remain
  - new vulnerabilities introduced