JOURNÉES NATIONALES 2018
PRÉ-GDR SÉCURITÉ INFORMATIQUE

CNRS

LA SÉCURITÉ DES MODEMS ET TERMINAUX MOBILES

Benoit MICHAU, ANSSI
benoit.michau[at]ssi.gouv.fr
31 mai 2018

Agence nationale de la sécurité
des systèmes d'information

ENVIRONNEMENT TECHNIQUE (1)

De nombreuses technologies de communications mobiles coexistent : 2G, 3G, 4G... 5G !

En France:

- appels, SMS : GSM (2G) et UMTS (3G)
- connexion de données : GPRS / EDGE (2G), UMTS / HSDPA / HSUPA (3G), LTE / LTE-A (4G)

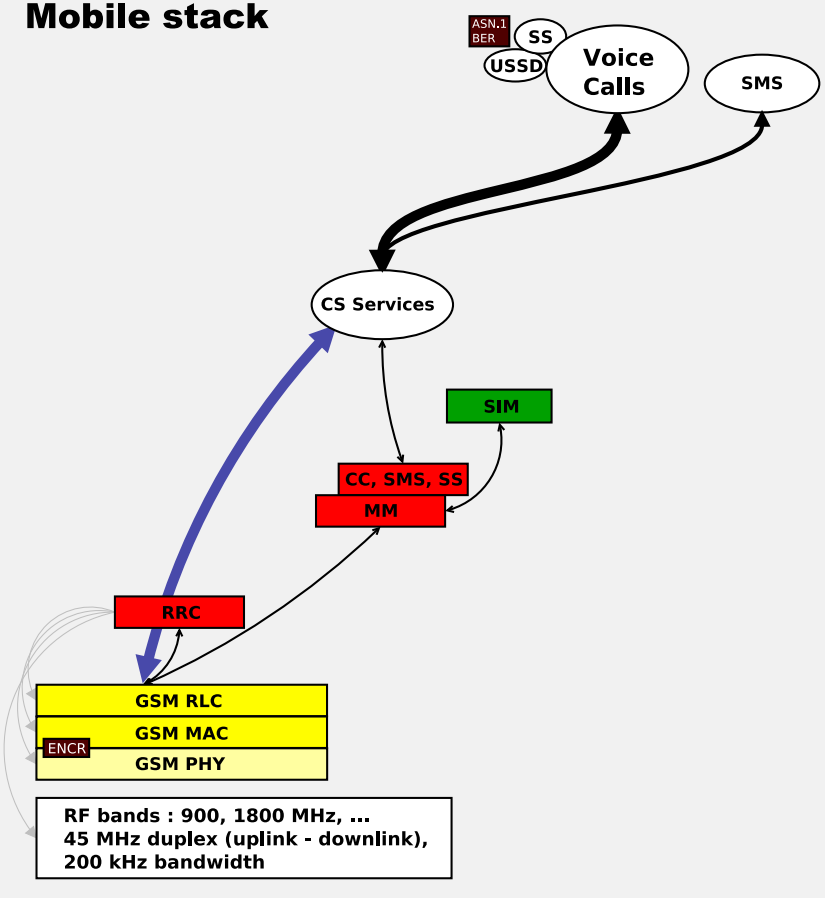
ENVIRONNEMENT TECHNIQUE (2)

La prise en charge des connexions cellulaires est complexe :

- multi-technologies et multi-fréquences
- fonctionne dans le monde entier
- multi-services
- mobilité
- économie d'énergie

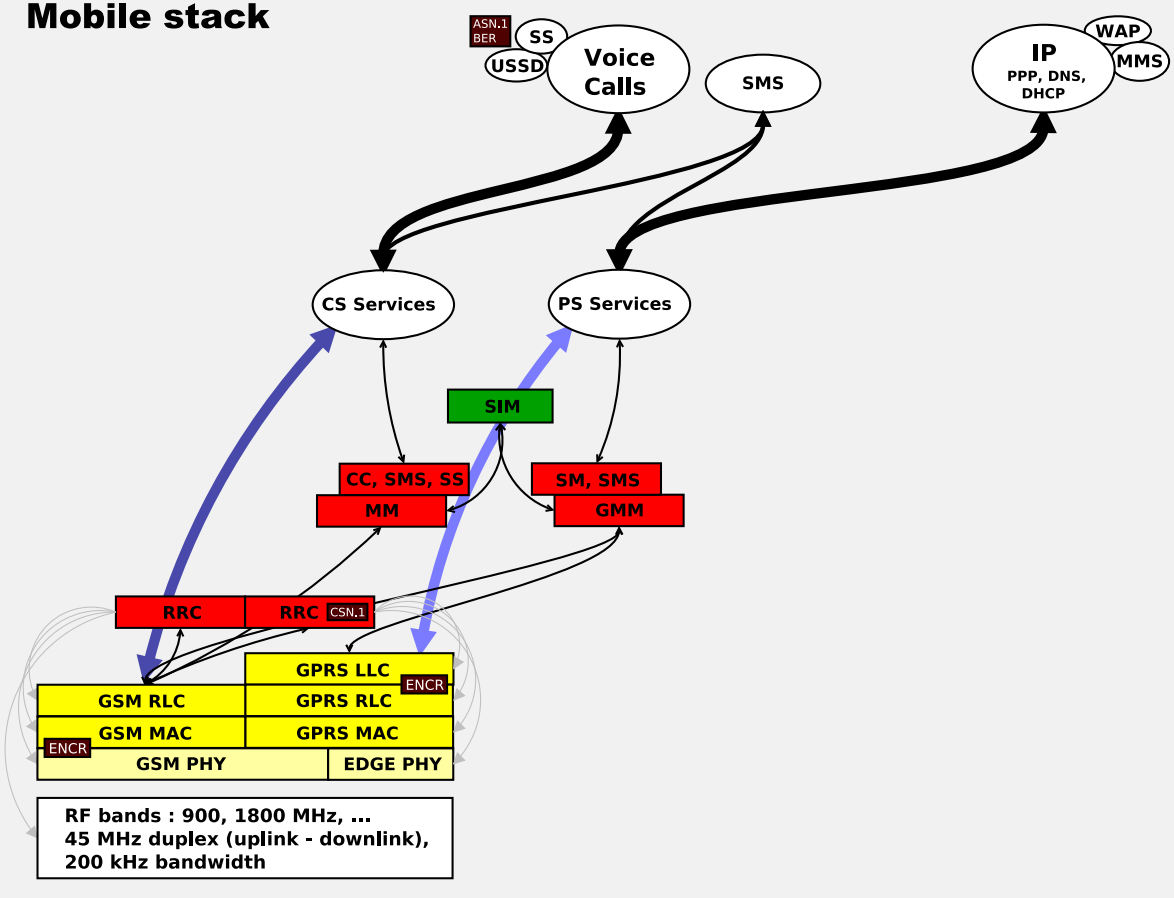
Processeur dédié (modem) : environnements matériel et logiciel fermés, indépendant ou intégré dans un SoC

Mobile stack



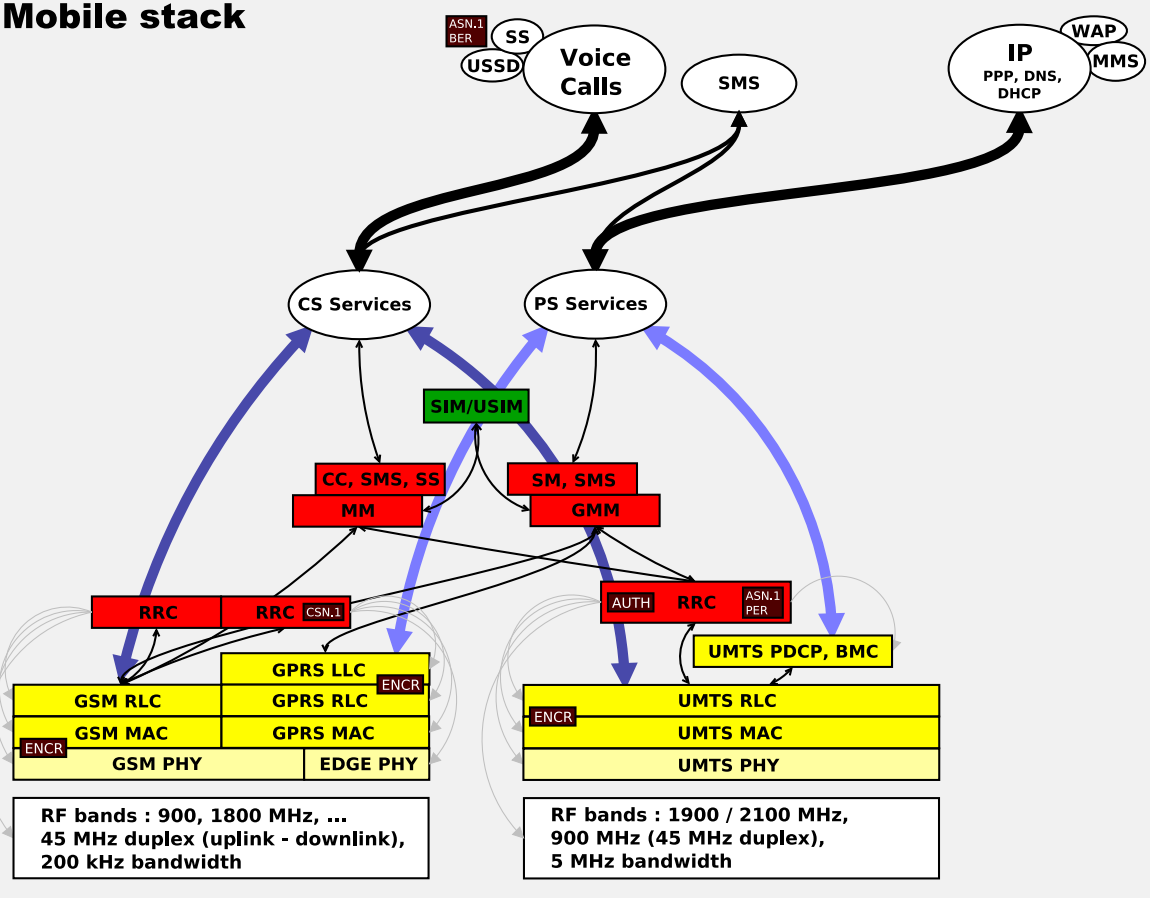
GSM stack

Mobile stack



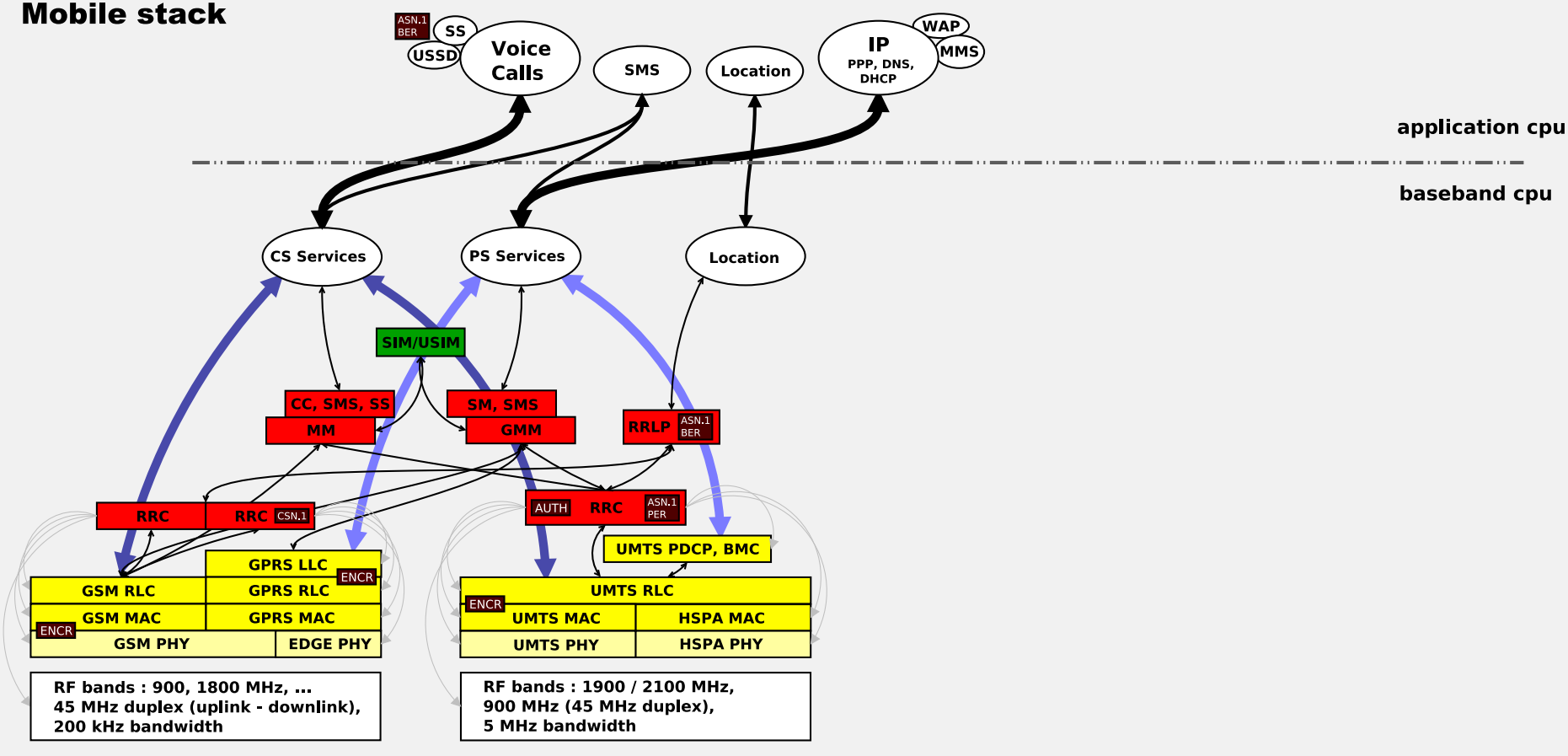
2G stack

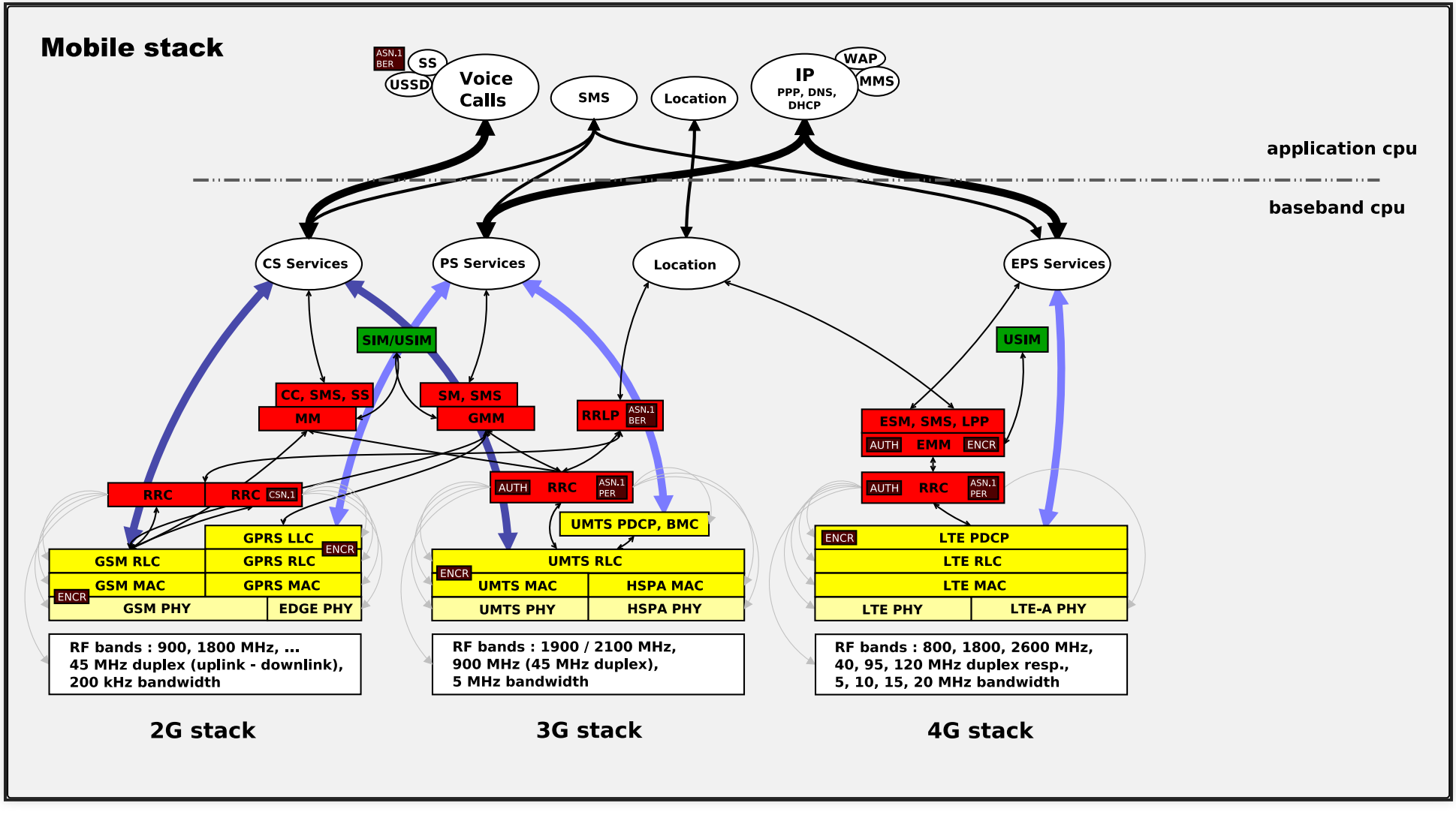
Mobile stack

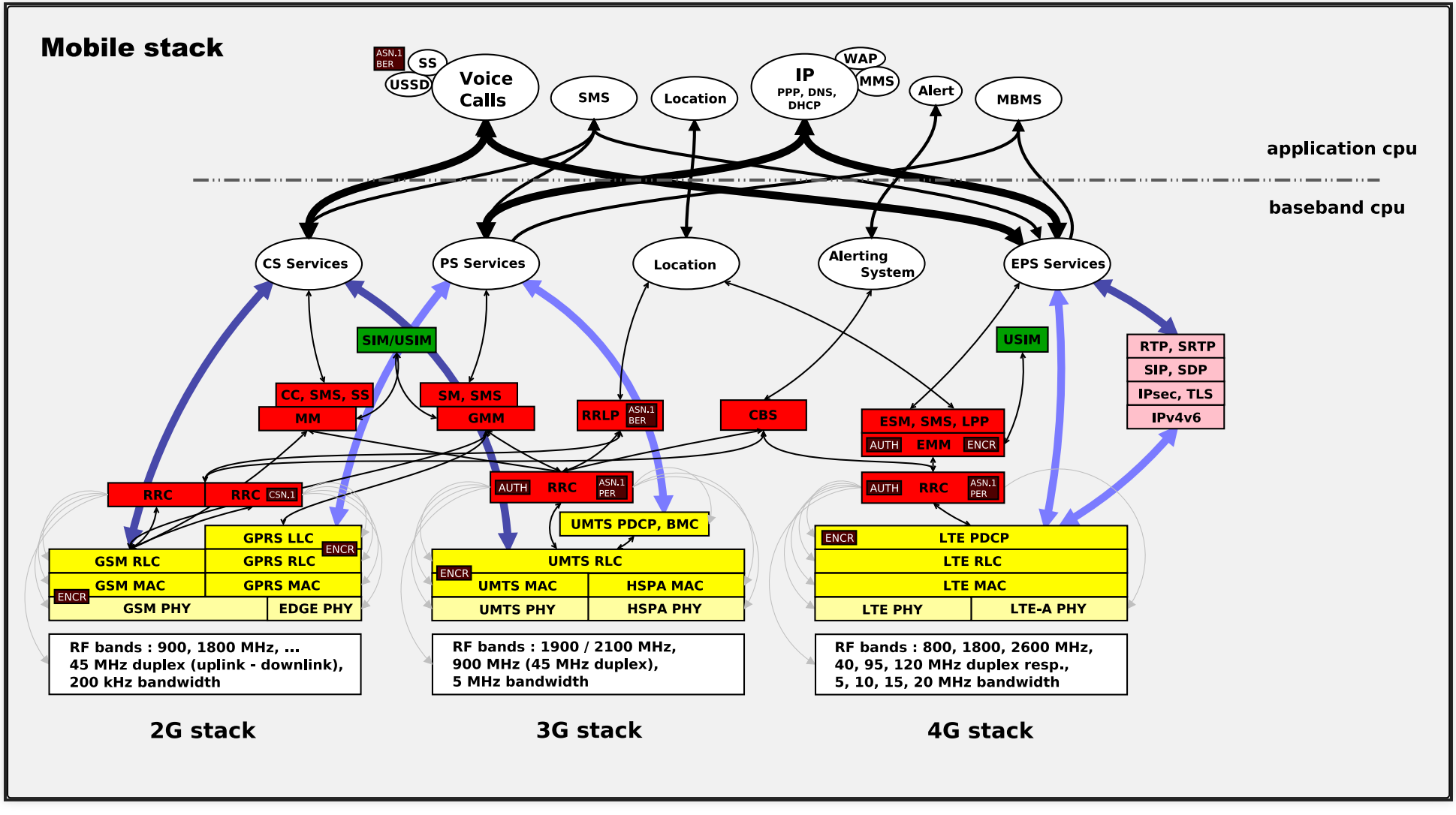


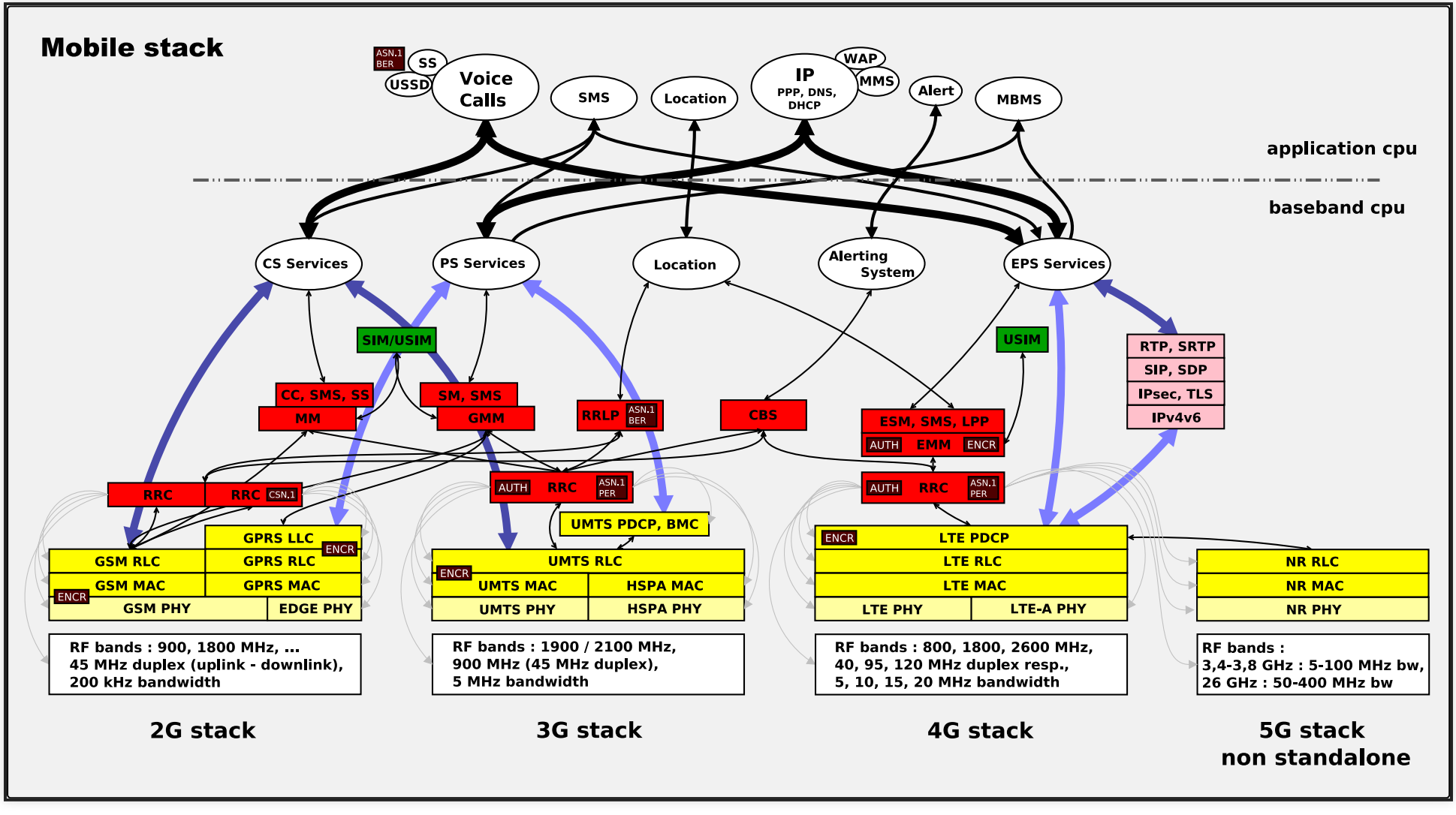
2G stack **3G stack**

Mobile stack




Mobile stack
ASN.1 BER
SS
USSD
Voice Calls
SMS
Location
IP
PPP, DNS, DHCP
WAP
MMS
application cpu
baseband cpu
CS Services
PS Services
Location
EPS Services
SIM/USIM
USIM
CC, SMS, SS
MM
SM, SMS
GMM
RRLP
ASN.1 BER
ESM, SMS, LPP
AUTH
EMM
ENCR
RRC
RRC
CSN.1
AUTH
RRC
ASN.1 PER
AUTH
RRC
ASN.1 PER
UMTS PDCP, BMC
GPRS LLC
ENCR
GSM RLC
GPRS RLC
GSM MAC
GPRS MAC
ENCR
GSM PHY
EDGE PHY
ENCR
UMTS RLC
ENCR
UMTS MAC
HSPA MAC
UMTS PHY
HSPA PHY
ENCR
LTE PDCP
LTE RLC
LTE MAC
LTE PHY
LTE-A PHY
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 : 800, 1800, 2600 MHz,
40, 95, 120 MHz duplex resp.,
5, 10, 15, 20 MHz bandwidth
2G stack
3G stack
4G stack


Mobile stack
ASN.1 BER
SS
USSD
Voice Calls
SMS
Location
IP
PPP, DNS, DHCP
WAP
MMS
Alert
MBMS
application cpu
baseband cpu
CS Services
PS Services
Location
Alerting System
EPS Services
SIM/USIM
USIM
RTP, SRTP
SIP, SDP
IPsec, TLS
IPv4v6
CC, SMS, SS
MM
SM, SMS
GMM
RRLP
ASN.1 BER
CBS
ESM, SMS, LPP
AUTH
EMM
ENCR
RRC
RRC
CSN.1
AUTH
RRC
ASN.1 PER
AUTH
RRC
ASN.1 PER
UMTS PDCP, BMC
GPRS LLC
ENCR
GSM RLC
GPRS RLC
GSM MAC
GPRS MAC
ENCR
GSM PHY
EDGE PHY
ENCR
UMTS RLC
ENCR
UMTS MAC
HSPA MAC
UMTS PHY
HSPA PHY
ENCR
LTE PDCP
LTE RLC
LTE MAC
LTE PHY
LTE-A PHY
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 : 800, 1800, 2600 MHz,
40, 95, 120 MHz duplex resp.,
5, 10, 15, 20 MHz bandwidth
2G stack
3G stack
4G stack


Mobile stack
ASN.1 BER
SS
USSD
Voice Calls
SMS
Location
IP
PPP, DNS, DHCP
WAP
MMS
Alert
MBMS
application cpu
baseband cpu
CS Services
PS Services
Location
Alerting System
EPS Services
SIM/USIM
USIM
RTP, SRTP
SIP, SDP
IPsec, TLS
IPv4v6
CC, SMS, SS
MM
SM, SMS
GMM
RRLP ASN.1 BER
CBS
ESM, SMS, LPP
AUTH EMM ENCR
RRC
RRC CSN.1
AUTH RRC ASN.1 PER
AUTH RRC ASN.1 PER
UMTS PDCP, BMC
GPRS LLC
ENCR
GSM RLC
GPRS RLC
GSM MAC
GPRS MAC
ENCR
GSM PHY
EDGE PHY
ENCR
UMTS RLC
ENCR
UMTS MAC
HSPA MAC
UMTS PHY
HSPA PHY
ENCR
LTE PDCP
LTE RLC
LTE MAC
LTE PHY
LTE-A PHY
NR RLC
NR MAC
NR PHY
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 : 800, 1800, 2600 MHz,
40, 95, 120 MHz duplex resp.,
5, 10, 15, 20 MHz bandwidth
RF bands :
3,4-3,8 GHz : 5-100 MHz bw,
26 GHz : 50-400 MHz bw
2G stack
3G stack
4G stack
5G stack
non standalone

FABRICANTS

- Qualcomm : smartphones, clés USB, principal fournisseur
- Mediatek : smartphones entrée de gamme
- Samsung : haut de gamme Samsung (sauf USA)
- HiSilicon : haut de gamme Huawei
- Intel (Infineon) : iPhone européens et asiatiques
- Spreadtrum : smartphones asiatiques
- les disparus : Sagem, Nokia, NVidia (Icera), Renesas, Broadcom, ST-Ericsson

SÉCURITÉ DES SERVICES MOBILES

services traités en clair dans le modem et le réseau opérateur :

- tous les services de téléphonie (appels, SMS, MMS...)
- les services de données transportés en clair (HTTP, SMTP...)

Egalement, configuration du terminal (OS applicatif, modem, carte SIM) par le réseau : heure, nom du réseau, paramètres de connexions de données, serveurs SMS, MMS...

SÉCURITÉ DES CONNEXIONS CELLULAIRES

- 2G : pas d'authentification du réseau, rend possible l'interception radio
- depuis la 3G : authentification mutuelle entre l'abonné et le réseau
- une partie des échanges radio demeure non-sécurisée :
  - canaux de diffusion descendant (cellules -> terminaux), y compris diffusion d'alertes sur cellule
  - canal montant de demande d'accès
  - amorce des connexions duplex entre cellules et terminaux

CONFIDENTIALITÉ DES CONNEXIONS CELLULAIRES

- 2G : chiffrement (LFSR avec clé de 64 bit)
- depuis la 3G : contrôle d'intégrité de la signalisation et chiffrement (algorithmes avec clé de 128 bit)
- réseau à l'initiative de la sélection de l'algorithme
- tous les terminaux acceptent des connexions sans chiffrement (sans notifier l'utilisateur)

SÉCURITÉ DU MODEM

Les firmwares des modems sont des exécutables complexes

- volumineux (>60 MO pour les modems Qualcomm récents)
- développés en C (éventuellement un peu de C++)
- en mode embarqué : pas de virtualisation mémoire, pas de séparation de privilèges, pas d'ASLR...
- certaines sections mémoire RWX
- éventuelle protection de la pile (Qualcomm)

EXEMPLES DE VULNÉRABILITÉS

SÉCURITÉ DES SERVICES MOBILES

- multiples vulnérabilités dans les cartes SIM et le «SIM-Toolkit» (2013)
- vulnérabilités d'un système de gestion à distance des terminaux (norme OMA-DM, 2014)
- nombreuses vulnérabilités dans la bibliothèque Android de traitement multimédia "libstagefright", déclenchable via MMS (2015)
- vulnérabilités régulières dans les gestionnaires de SMS, MMS, WAP-Push...

SÉCURITÉ DES CONNEXIONS CELLULAIRES

- projet OpenBTS : permet d'attacher n'importe quel terminal 2G, disponible depuis 2007
- compromission de femtocells 3G : permet d'accéder à l'ensemble des communications cellulaires 3G (entre 2011 et 2015)
- contournements des mécanismes d'activation de la sécurité des connexions 3G et 4G des modems (2016)

CONFIDENTIALITÉ DES CONNEXIONS CELLULAIRES

- Cryptanalyse de l'algorithme de chiffrement GSM A5/1 (2009)
- Données de signalisation LTE non confidentielles (IMSI, geolocalisation..., 2015) et rabaissement possible vers un réseau 2G (2016)

EXPLOITATION DE CORRUPTIONS MÉMOIRES (1)

- exploitation de vulnérabilités dans les modems Intel et Qualcomm (2012) : activation de la prise d'appel automatique
- exploitation d'un débordement de pile dans le gestionnaire d'appel GSM des modems Samsung (2015) : reroute les appels sortants
- multiples corruptions mémoire lors du traitement de messages d'alerte diffusés (2018)

EXPLOITATION DE CORRUPTIONS MÉMOIRES (2)

- exploitation d'un débordement de pile dans le gestionnaire de sessions GPRS des modems Samsung (2017) : écriture de fichiers sur la carte SD
- exploitation d'un débordement de pile dans les modems HiSilicon (2017) : ré-écriture de l'IMEI du terminal
- exploitations de corruptions mémoire dans les firmwares des chipsets Wi-Fi Broadcom et élévations de privilèges dans le noyau Android et le noyau iPhone OS (2017)

L'IMPORTANCE D'ÉVALUER LA SÉCURITÉ DES MODEMS (1)

Les modems cellulaires sont partout : téléphones, smartphones, voitures, drônes, automates commerciaux ou industriels, équipements connectés...

Ils présentent une surface d'exposition importante : actifs en permanence, décodage opportuniste de signaux radio complexes, interactions importantes avec les applicatifs...

Ils traitent une grande partie des communications entrantes et sortantes, en partie en clair.

L'IMPORTANCE D'ÉVALUER LA SÉCURITÉ DES MODEMS (2)

Leur fonctionnement est totalement opaque vis-à-vis de l'utilisateur.

Leur évaluation en «boîte noire» est délicate.

Peu de contre-mesures modernes aux corruptions mémoire y sont intégrées.

L'ÉVALUATION DANS LES FAITS

Utiliser des simulateurs de réseaux open-source (OpenBTS / YateBTS, osmocom, srs-lte, OAI, corenet, NextEPC) ou commerciaux (amarisoft, corenet dynamics) pour créer et tester des situations extrêmes ou hors-normes (prévoir une isolation RF).

Analyser le fonctionnement des modems et terminaux mobiles (adb, systèmes de diagnostic des modems, analyse statique des firmwares, ram-dumps, crash-dumps).

LES DOMAINES D'EXPERTISE

- protocoles (modulation radio, ASN.1)
- cryptographie (primitives principalement symétriques, schémas d'authentification et de dérivation de clés)
- retro-ingénierie de systèmes embarqués (ARM, Hexagon)
- ingénierie (compréhension des normes de téléphonie mobile, développement logiciel)
- carte à puce (SIM)

LES RÉPONSES AUX PROBLÈMES

LES FABRICANTS DE MODEMS

Les grands fabricants ont des équipes dédiées :
Qualcomm, Samsung, Huawei, Google, Apple...
Les plus petits sont généralement plus difficiles à contacter, ou sensibiliser.
Distribution des mises à jour et maintenance des firmwares rarement parfaites.

LES OPÉRATEURS MOBILES

Introduction d'A5/3 (chiffrement GSM).
Abandon des réseaux 2G (exemple d'AT&T).
Surveillance des interfaces de roaming inter-opérateurs.

LES ABONNÉS MOBILES

Maintenir ses terminaux à jour, autant que possible.

CONCLUSION

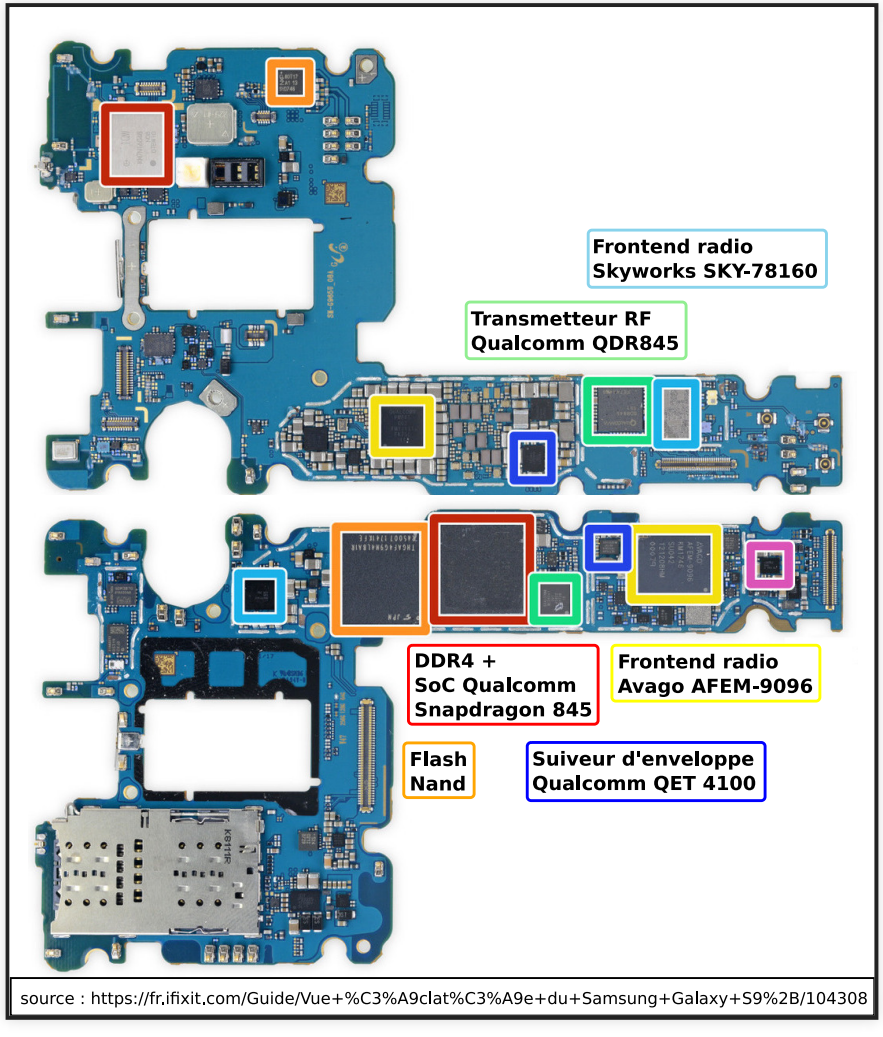
Les grands fabricants et éditeurs améliorent sans cesse la sécurité de leurs produits.
Malheureusement, la sécurité des modems reste généralement en-deçà de l'état de l'art, et les technologies cellulaires évoluent sans cesse.
C'est un domaine de recherche en sécurité informatique à part entière.

N'hésitez pas à vous y interesser !

ANNEXE

Exemples de mises en oeuvre hardware

SAMSUNG GALAXY S9+ (QUALCOMM)

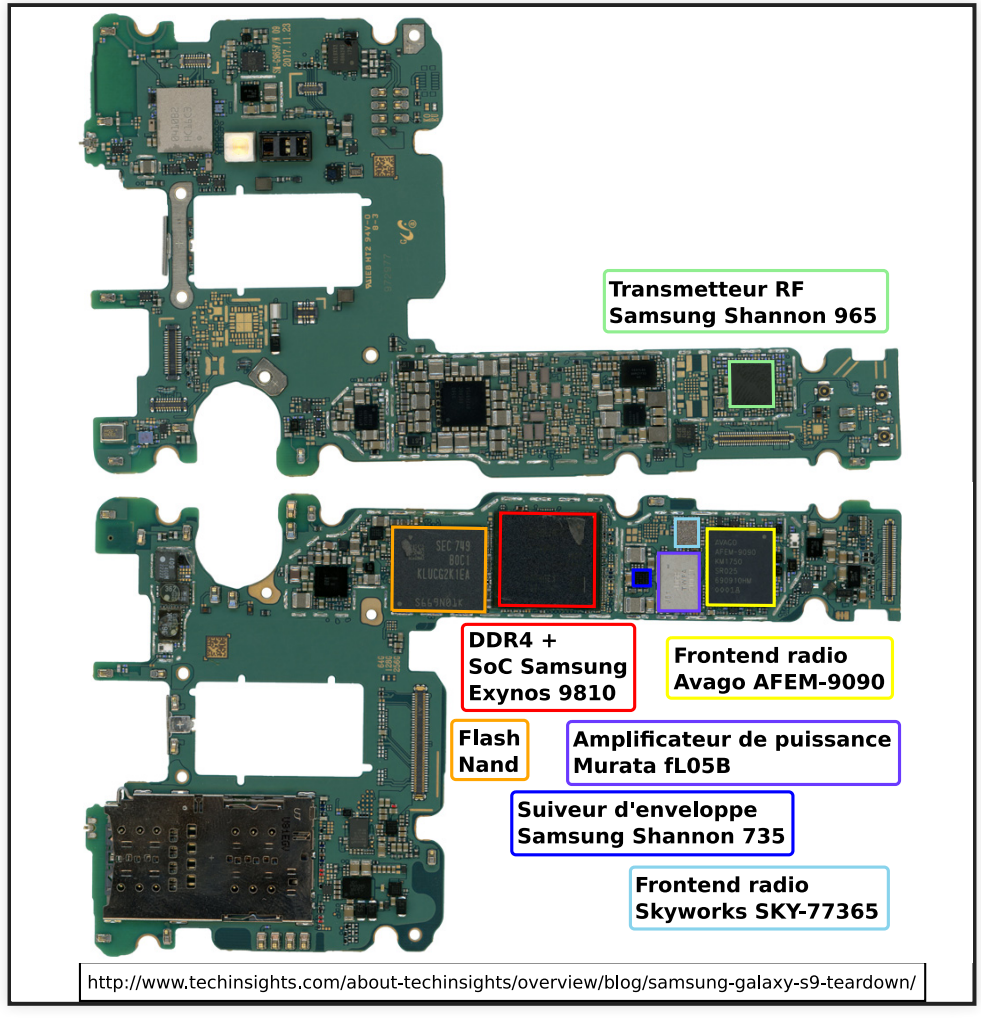


démontage d'un Galaxy S9+ (QC)

ARCHITECTURE MATÉRIELLE SOC

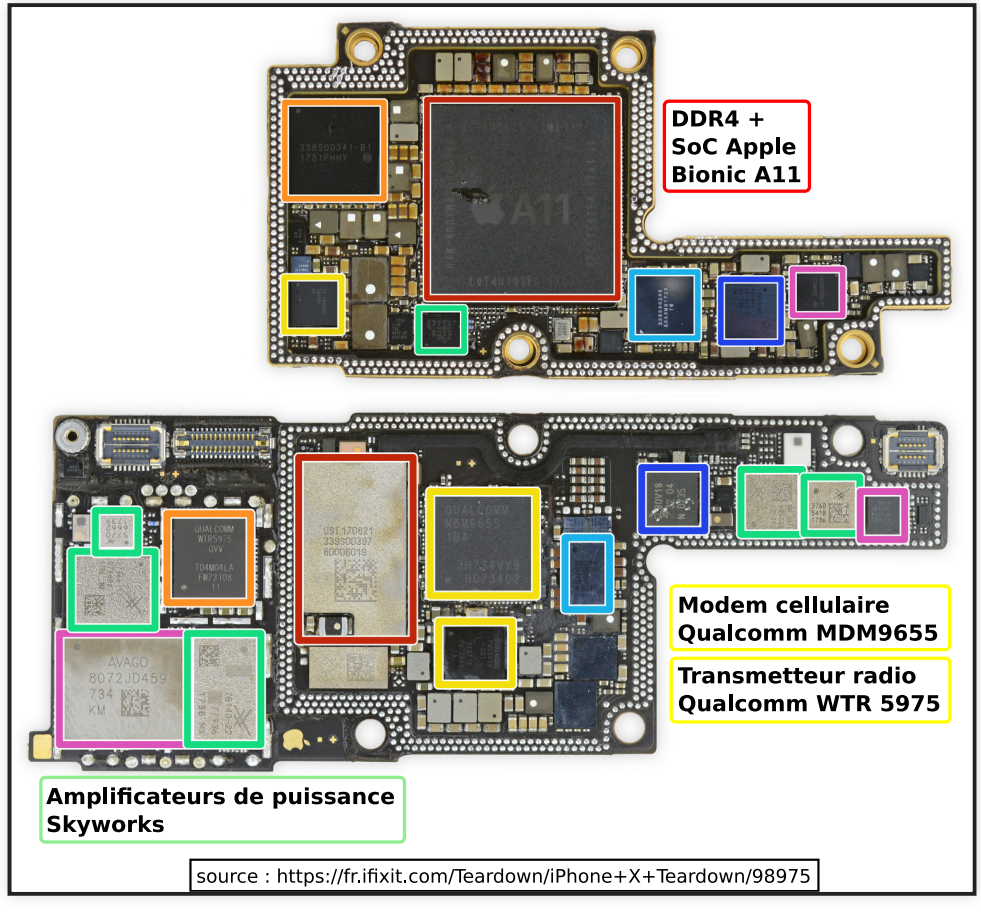
SoC Qualcomm:
- RAM partagée pour l'ensemble des modules du SoC (isolation via MPU)
- émulation de liaisons série entre le modem et le processeur applicatif via une zone mémoire partagée
- modem entièrement exécuté sur DSP Hexagon
- basé sur un OS temps réel propriétaire Qualcomm

SAMSUNG GALAXY S9+ (SAMSUNG)



démontage d'un Galaxy S9+ (SS)

IPHONE X (QUALCOMM)



démontage d'un iPhone X (QC)

ARCHITECTURE MATÉRIELLE IPHONE

iPhone avec modem Qualcomm:
- puce indépendante (RAM, coeur ARM et DSP Hexagon) interconnectée avec le processeur applicatif en PCIe
- modem entièrement exécuté sur DSP Hexagon (idem SoC Qualcomm)

iPhone avec modem Intel:
- puce indédendante (RAM, coeur ARM et DSP) interconnectée avec le processeur applicatif en SSIC (USB3 sur PCB)
- modem essentiellement exécuté sur le coeur ARM
- basé sur un OS temps réel ThreadX

ARCHITECTURE MATÉRIELLE MODEM USB

TODO

AUTRES RESSOURCES

présentation du Samsung Galaxy S9+ (QC et SS)
présentation de l'iPhone 8 (QC et Intel)
démontage d'un iPhone 8 (Intel)
démontagd d'un iPhone 8 (QC)
présentation du SoC Qualcomm Snapdragon 845
réference technique du SoC applicatif Snapdragon 820e (sans modem) réference technique du SoC applicatif Snapdragon 410e (sans modem)