Recherche sur la sécurité des baseband (QC) en 2024

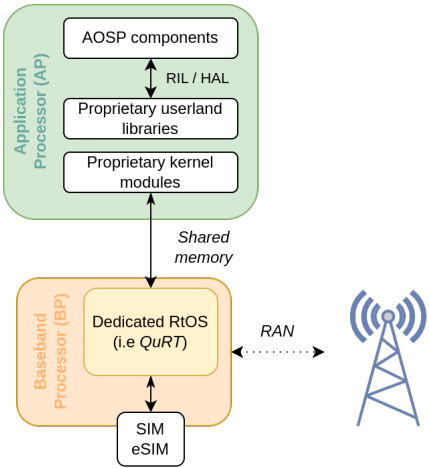
Finalement j'arrête tout

Florian Le Minoux (@flogallium)

Bière Sécu Rennes, 12 novembre 2024

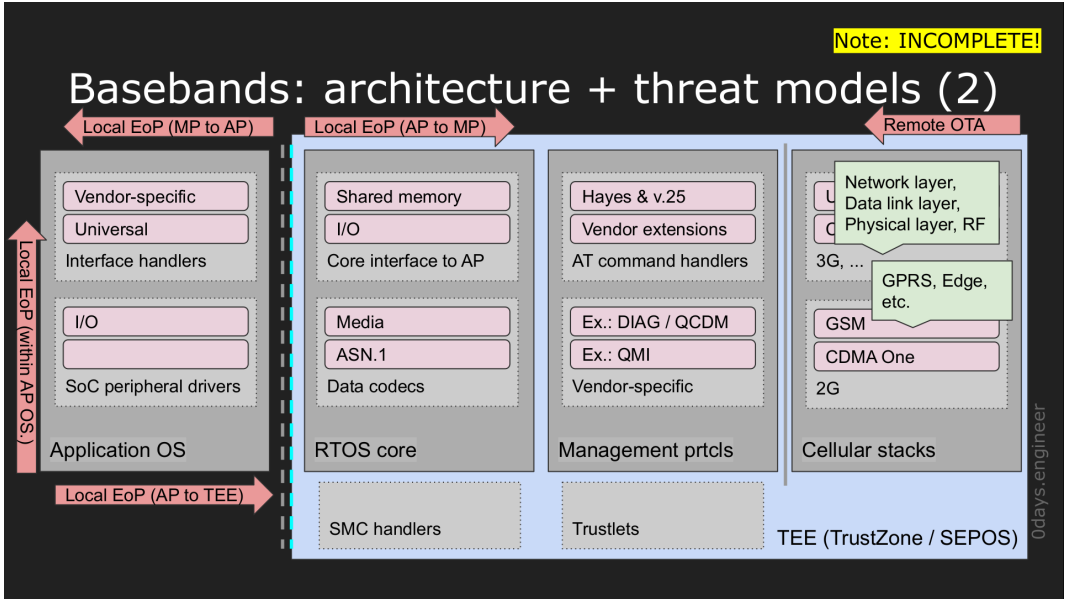
Baseband

- Processeur indépendant du processeur principal (AP) mais communicant avec lui pour gérer toute la téléphonie (modulation et la partie protocolaire) : GPRS/EDGE/CDMA/LTE/5G...
- Forte concentration des fabriquants et des firmwares :
  - Leaders : **Qualcomm** (iPhone, Pixel) et Samsung
  - Huawei, Mediatek



Objectif

- On ne parle pas assez de Baseband !
- Mieux comprendre son fonctionnement et sa surface.
- Documenter plus le fonctionnement de la plateforme Qualcomm et la recherche pour ce type de plateforme.



https://alisa.sh/slides/AdvancedHexagonDiag.pdf

Baseband Qualcomm

Les baseband Qualcomm récents tournent sur un DSP [1] dédié, reposant sur une ISA maison nommée **Hexagon** et faisant tourner un RTOS maison nommé **QuRT**.

- Firmware en clair (mais protégé par TZ)
- DEP, stack cookies
- Pas d'ASLR, adresses hardcodées partout

1. Digital Signal Processor

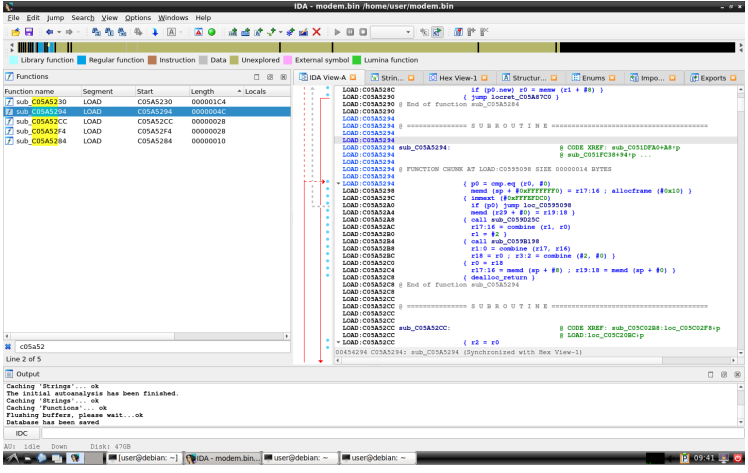
Firmware du baseband : reverse

- Pour les Pixel, firmware récupérable sur le site de Google.
- Plusieurs étapes pour unpack le firmware au format ELF [2].
- QC rends les choses compliquées avec de la décompression matérielle à la volée (CLADE) et de l'obfu des strings de debug (remplacées par leur MD5 fournis dans un autre fichier) [3].
- Assez peu de leak internes utiles sauf ça [4]

2. https://github.com/anestisb/qc_image_unpacker
3. https://github.com/mzakocs/qualcomm_baseband_scripts
4. https://gitlab.com/qcom-sources15/msm8916_2014-12-03_amss_qrd/

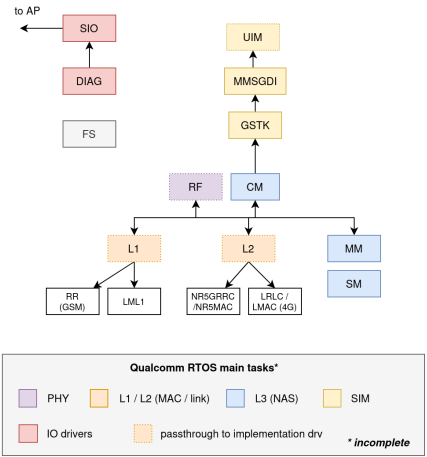
Firmware du baseband : reverse

En utilisant IDA 8.2 et `https://github.com/gsmk/hexagon`.



Firmware du baseband : reverse

- Le firmware est organisé en tâches. Des tâches spécialisées dans une techno (LMAC pour la 4G) appelées par des tâches génériques (L2).
- Les parsers sont dans des fonctions dédiées (préfixées `ps_`), le firmware contient beaucoup de parsers (PPP/IP46/IPSec/Http/Xml/IPSec/SIP/EAP...)
- Il contient aussi une Stack TCP et TLS
- Les services d'IO est sont dans des fonctions dédiées (préfixées `ds_`)



Debugging

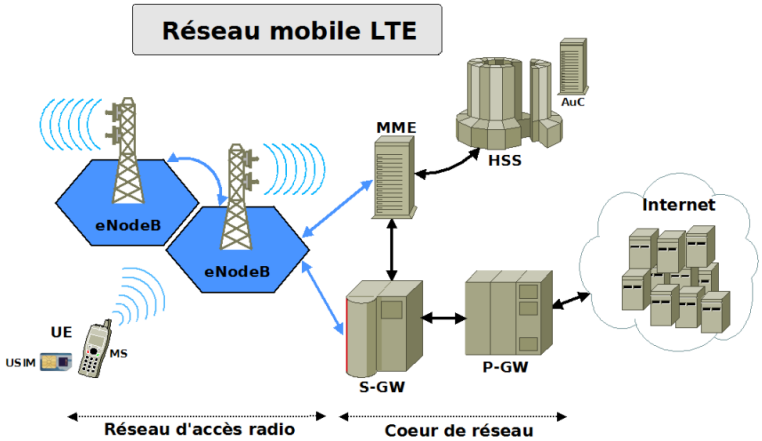
- Protocole DIAG propriétaire de Qualcomm :
  - Assez peu documenté et documentation en partie obsolète [5]
  - Récupération d'un logging (très) verbose possible [6] et GSMTAP [7]
  - Pas de crashdumps / pas de RW sur les chips de production
  - Leaks de tools internes à QC : QPST/QXDM
- Émulation : archi dispo sur QEMU mais émulation uniquement userland
- Patch : pas possible, firmware signé et vérifié par TrustZone

5. https://fahrplan.events.ccc.de/congress/2011/Fahrplan/attachments/2022_11-ccc-qcombbdbg.pdf
6. https://alisa.sh/slides/AdvancedHexagonDiag.pdf
7. https://github.com/P1sec/QCSuper

Exploitation

- Principale cible : protocoles OTA depuis réseau controllé
- CVE fréquentes mais l'intitulé est souvent vague et quasiment jamais de PoC / 1day publiques.

Infrastructure LTE



https://cyber.gouv.fr/sites/default/files/IMG/pdf/Benoit_Michau_-_Securite_des_modems_des_terminaux_mobiles.pdf

Infrastructure LTE

- **eNodeB** : *base station* LTE
- **HSS**, *Home Subscriber Server* : base de donnée abonnés (IMSI/MSISDN/secrets SIM), gère l'authentification UE-réseau
- **MME**, *Mobile Management Entity* : gestion de la signalisation, "cache régional du HSS", protocole NAS
- **IMS**, *IP Multimedia Subsystem* : standardisation IP des protocoles historiquements commutés (voix/SMS) : protocoles SIP/RTP, Diameter...

Infrastructure LTE

- Un femtocell documenté ou une radio logicielle (SDR) full-duplex (limeSDR/bladeRF/USRP) et du soft d'émission
- Un coeur de réseau LTE contenant HSS, PGW/SGW, MME
  - srsRAN 4G
  - Open5GS
  - OpenAirInterface
  - corenet

  $\rightarrow$ Utilisez docker-open5gs [8] !
- SIM dont le secret est connu : *sysmoISIM* ou profil eSIM de test [9] (marche sur certains combo device/BB, i.e. Pixel)

8. `https://github.com/herlesupreeth/docker_open5gs`
9. `https://source.android.com/docs/core/connect/esim-test-profiles`

Surfaces OTA intéressantes

- SIP/SDP
  - HTTP like, peut contenir du XML, parsé par le BB
  - Plus facile à fuzz/craft
  - Passif de vulns chez Samsung [10] [11] et QC [12]

10. https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Over-The-Air-Baseband-Exploit-Gaining-Remote-Code-Execution-On-5G-Smartphones.pdf
11. https://hardwear.io/usa-2023/presentation/how-to-hack-shannon-baseband.pdf
12. https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2024-bulletin.html

Surfaces OTA intéressantes

- XCAP [13]
  - Protocole de configuration gérant notamment le renvoi d'appel
  - HTTP + XML, parsé par le BB

13. https://realtimecommunication.wordpress.com/2015/05/27/ut-interface-what-is-it-for/

Surfaces OTA intéressantes

- Signaling / NAS
  - Protocoles TLV adhoc compliqués mais régulièrement vulnérables [a]
  - Nécessite de lire les standards GSMA/ETSI (éprouvant)
  - Nécessite de patcher la suite de radio utilisée

Table 8.2.1.1: ATTACH ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach accept message identity	Message type 9.8	M	V	1
	EPS attach result	EPS attach result 9.9.3.10	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	M	V	1/2
	T3412 value	GPRS timer 9.9.3.16	M	V	1
	TAI list	Tracking area identity list 9.9.3.33	M	LV	7-97
	ESM message container	ESM message container 9.9.3.15	M	LV-E	5-n
50	GUTI	EPS mobile identity 9.9.3.12	O	TLV	13
13	Location area identification	Location area identification 9.9.2.2	O	TV	6
23	MS identity	Mobile identity 9.9.2.3	O	TLV	7-10
53	EMM cause	EMM cause 9.9.3.9	O	TV	2
17	T3402 value	GPRS timer 9.9.3.16	O	TV	2
59	T3423 value	GPRS timer 9.9.3.16	O	TV	2
4A	Equivalent PLMNs	PLMN list 9.9.2.8	O	TLV	5-47
34	Emergency number list	Emergency number list 9.9.3.37	O	TLV	5-50
64	EPS network feature support	EPS network feature support 9.9.3.12A	O	TLV	3-4
F-	Additional update result	Additional update result 9.9.3.0A	O	TV	1
5E	T3412 extended value	GPRS timer 3 9.9.3.16B	O	TLV	3
6A	T3324 value	GPRS timer 2 9.9.3.16A	O	TLV	3
6E	Extended DRX parameters	Extended DRX parameters 9.9.3.46	O	TLV	3
65	DCN-ID	DCN-ID 9.9.3.48	O	TLV	4
E-	SMS services status	SMS services status 9.9.3.4B	O	TV	1
D-	Non-3GPP NW provided policies	Non-3GPP NW provided policies 9.9.3.49	O	TV	1
6B	T3448 value	GPRS timer 2 9.9.3.16A	O	TLV	3
C-	Network policy	Network policy 9.9.3.52	O	TV	1
6C	T3447 value	GPRS timer 3 9.9.3.16B	O	TLV	3
7A	Extended emergency number list	Extended emergency number list 9.9.3.37A	O	TLV-E	6-65538
7C	Ciphering key data	Ciphering key data 9.9.3.56	O	TLV-E	35-2291

a. `https://docs.qualcomm.com/product/publicresources/securitybulletin/august-2024-bulletin.html`

Surfaces OTA intéressantes

- Attaque depuis la carte SIM
  - Les SIMs peuvent contenir des applets Javacard [14]
  - Ces applets utilisent l'API STK qui communique avec le téléphone via le baseband (affichage de vieux menus, lancement d'appels/pages web...)
  - Peuvent être envoyés en OTA via un SMS silencieux

14. https://speakerd.s3.amazonaws.com/presentations/3f6019d0e0ff013010f03ed23fede438/SIM_Toolkit.pdf

Surfaces spécifiques à QC

- QMI [15] et DIAG [16] depuis le téléphone (driver SMD)

15. https://research.checkpoint.com/2021/security-probe-of-qualcomm-msm/
16. https://alisa.sh/slides/AdvancedHexagonDiag.pdf

Conclusion

- **J'ai rien trouvé !**
- Coût important de rentrer dans le monde de la téléphonie et ses 30 ans de *legacy*
- QC reste la plateforme BB la plus dure à attaquer du fait de son architecture/hardening et ça se ressent sur la littérature
- Ma contribution à part ce blabla : `https://github.com/darkgallium/qcbb`

Ressources utiles

- nickvsnetworking.com
- realtimecommunication.wordpress.com
- howltestuffworks.blogspot.com

Merci de votre attention !