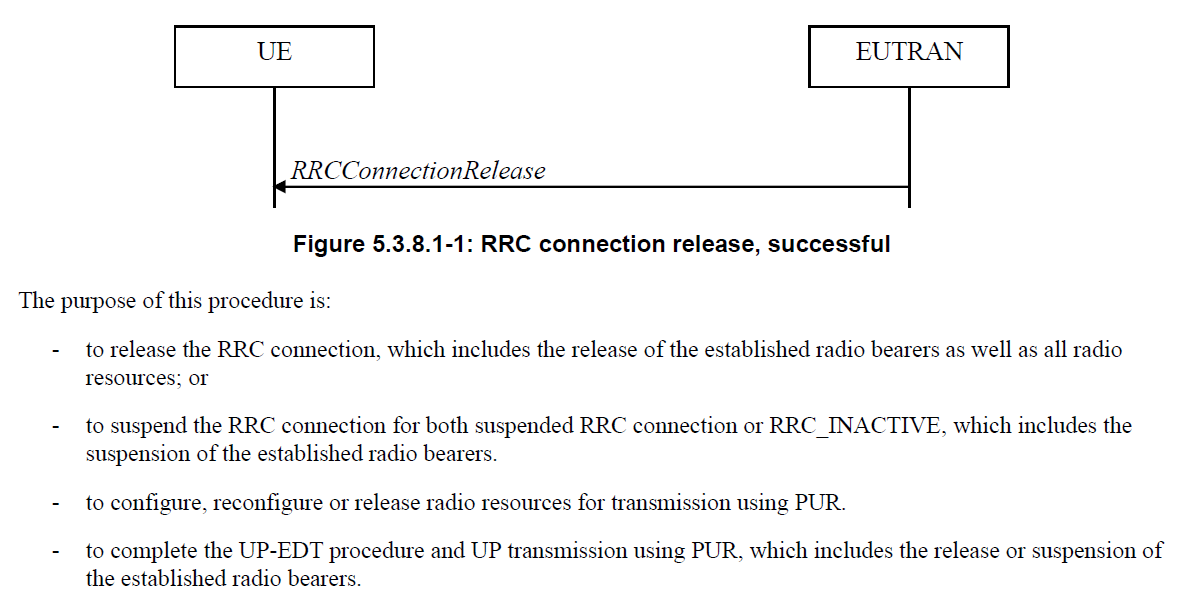
**LTE RRCConnectionRelease Redirect (analyse du problème)**

Ce problème a été découvert et soulevé par des chercheurs nationaux en 2016, et une attaque complète a été mise en œuvre. Parce qu'il s'agit d'un problème très classique, il est également nécessaire de le reproduire dans le processus d'apprentissage de la sécurité LTE/5G. J'ai probablement reproduit ce problème au début de cette année.

RRCConnectionRelease En 5GNR oui RRCRelease.

RRCConnectionRelease L'utilisation normale est :



Envoyé par la station de base à l'UE, le rôle comprend la libération d'un rrc connection…

Fondamental :

Lorsque la couche nas rejette la connexion actuelle et que l'UE la reçoit, elle déclenchera l'envoi par la station de base du message rrcconnectionrelease à l'UE. À ce moment, l'UE analysera le paquet rrcconnectionrelease, car la connexion elle-même est également le problème. rrcconnectionrelease sera déclenché, c'est-à-dire que la couche de station de base peut être perdue.La clé et d'autres informations pour l'enregistrement sur le réseau au début. Par conséquent, comme décrit au début du protocole, l'UE ne vérifie pas l'intégrité du rrcconnectionrelease après l'avoir reçu, mais le reçoit et l'analyse directement.

La structure redirectedCarrierInfo peut être transportée dans rrcconnectionrelease, et vous pouvez voir directement la définition de la structure dans le fichier asn :

typedef struct LTE\_RRCConnectionRelease\_r8\_IEs {  
 LTE\_ReleaseCause\_t releaseCause;  
 struct LTE\_RedirectedCarrierInfo \*redirectedCarrierInfo; /\* OPTIONAL \*/  
 struct LTE\_IdleModeMobilityControlInfo \*idleModeMobilityControlInfo; /\* OPTIONAL \*/  
 struct LTE\_RRCConnectionRelease\_v890\_IEs \*nonCriticalExtension; /\* OPTIONAL \*/  
   
 /\* Context for parsing across buffer boundaries \*/  
 asn\_struct\_ctx\_t \_asn\_ctx;  
} LTE\_RRCConnectionRelease\_r8\_IEs\_t;  
//////  
typedef enum LTE\_RedirectedCarrierInfo\_PR {  
 LTE\_RedirectedCarrierInfo\_PR\_NOTHING, /\* No components present \*/  
 LTE\_RedirectedCarrierInfo\_PR\_eutra,  
 LTE\_RedirectedCarrierInfo\_PR\_geran,  
 LTE\_RedirectedCarrierInfo\_PR\_utra\_FDD,  
 LTE\_RedirectedCarrierInfo\_PR\_utra\_TDD,  
 LTE\_RedirectedCarrierInfo\_PR\_cdma2000\_HRPD,  
 LTE\_RedirectedCarrierInfo\_PR\_cdma2000\_1xRTT,  
 /\* Extensions may appear below \*/  
 LTE\_RedirectedCarrierInfo\_PR\_utra\_TDD\_r10,  
 LTE\_RedirectedCarrierInfo\_PR\_nr\_r15  
} LTE\_RedirectedCarrierInfo\_PR;  
//////  
typedef struct LTE\_RedirectedCarrierInfo {  
 LTE\_RedirectedCarrierInfo\_PR present;  
 union LTE\_RedirectedCarrierInfo\_u {  
 LTE\_ARFCN\_ValueEUTRA\_t eutra;  
 LTE\_CarrierFreqsGERAN\_t geran;  
 LTE\_ARFCN\_ValueUTRA\_t utra\_FDD;  
 LTE\_ARFCN\_ValueUTRA\_t utra\_TDD;  
 LTE\_CarrierFreqCDMA2000\_t cdma2000\_HRPD;  
 LTE\_CarrierFreqCDMA2000\_t cdma2000\_1xRTT;  
 /\*  
 \* This type is extensible,  
 \* possible extensions are below.  
 \*/  
 LTE\_CarrierFreqListUTRA\_TDD\_r10\_t utra\_TDD\_r10;  
 LTE\_CarrierInfoNR\_r15\_t nr\_r15;  
 } choice;  
   
 /\* Context for parsing across buffer boundaries \*/  
 asn\_struct\_ctx\_t \_asn\_ctx;  
} LTE\_RedirectedCarrierInfo\_t;

On peut constater que redirectedCarrierInfo fournit en fait à l'UE une ou plusieurs fréquences/canaux/arfcn optionnels. Lorsque l'UE le reçoit, il sélectionne une cellule appropriée en fonction des informations. (La procédure peut également être utilisée pour libérer et rediriger un UE vers une autre fréquence)

alentours

Cela n'affecte pas le réseau existant, utilisez donc oai et openair-cn pour créer un réseau LTE. Connectez-vous avec un téléphone mobile normal (UE). (Ordinateur portable USRP B210+)

Le choix est de déclencher le RRCConnectionRelease de la station de base via le rejet d'attachement envoyé par le cœur de réseau/MME.

Dans le test d'état initial, utilisez la cause 17 pour le rejet de connexion, la défaillance du réseau, une cause relativement "faible".

Le code oai ne change pas et le redirectedCarrierInfo n'est pas transporté dans le RRCConnectionRelease par défaut. Modifiez openair-cn, lors de la réception de la première demande de rattachement, envoyez un refus de rattachement, cause 17 ; et la deuxième fois traitera la demande de rattachement (c'est-à-dire accepter) normalement.

Construisez un environnement 2G et faites-le fonctionner. (une machine virtuelle Linux + limesdr mini)

Phénomène : Après le premier rejet d'attachement, l'UE continue d'initier une demande d'attachement au réseau LTE, puis se connecte normalement au réseau LTE.

**Ajouter redirected carrierinfo**

Dans oai existe asn1\_msg.c au milieu, do\_RRCConnectionRelease Il est utilisé pour construire le package RRCConnectionRelease et ajouter la structure redirectedCarrierInfo. Par exemple mon ajout :

LTE\_RedirectedCarrierInfo\_t rInfo;  
   
 // geran  
 rInfo.present = LTE\_RedirectedCarrierInfo\_PR\_geran;  
 LTE\_CarrierFreqsGERAN\_t cfgt;  
 cfgt.startingARFCN = 636;  
 cfgt.bandIndicator = 0;  
 cfgt.followingARFCNs.present = LTE\_CarrierFreqsGERAN\_\_followingARFCNs\_PR\_equallySpacedARFCNs;  
 cfgt.followingARFCNs.choice.equallySpacedARFCNs.arfcn\_Spacing = 1;  
 cfgt.followingARFCNs.choice.equallySpacedARFCNs.numberOfFollowingARFCNs = 0;  
  
 rInfo.choice.geran = cfgt;  
  
......  
 rrcConnectionRelease->criticalExtensions.choice.c1.choice.rrcConnectionRelease\_r8.redirectedCarrierInfo = &rInfo;

La correspondance entre arfcn et fréquence peut être référencée, il suffit de la maintenir cohérente avec la pseudo station de base que vous avez construite :

https://wenku.baidu.com/view/55e2d6677cd184254a35355b.html

Le phénomène est qu'il est directement connecté à la pseudo station de base 2G construite après un rejet d'attachement.

A suivre

Un problème découvert très tôt, mais un correctif a été ajouté très tard dans la documentation du protocole 3GPP. Un téléphone portable de la fin du 19 utilisé pour les tests est également concerné.

Lorsque l'UE reçoit RCCConnectionRelease/RRCRelease, 36331 et 38331 dans le flux de traitement ont des modifications pertinentes. Par exemple, 36331 est décrit comme suit :

1> if the RRCConnectionRelease message includes redirectedCarrierInfo indicating redirection to geran:  
 2> if AS security has not been activated, and   
 2> if upper layers indicate that redirect to GERAN without AS security is not allowed:  
 3> perform the actions upon leaving RRC\_CONNECTED as specified in 5.3.12, with release cause 'other', upon which the procedure ends;

1> if the RRCConnectionRelease message includes redirectedCarrierInfo indicating redirection to geran; or  
1> if the RRCConnectionRelease message includes idleModeMobilityControlInfo including freqPriorityListGERAN:  
 2> if AS security has not been activated; and  
 2> if upper layers indicate that redirect to GERAN without AS security is not allowed:  
 3> ignore the content of the RRCConnectionRelease;  
 3> perform the actions upon leaving RRC\_CONNECTED or RRC\_INACTIVE as specified in 5.3.12, with release cause 'other', upon which the procedure ends;

La description doit avoir une protection d'intégrité après AS Security ; si elle est avant AS Security, le champ redirectedCarrierInfo ne sera pas traité. En fait, il existe également une telle condition si les couches supérieures indiquent qu'elles redirigent vers GERAN, cela a donc beaucoup à voir avec la mise en œuvre de la bande de base.

Dans 38331, un ignorer supplémentaire a été ajouté à la version 15.6.0 (19 juin) :

1> if the AS security is not activated:  
 2> ignore any field included in RRCRelease message except waitTime;  
 2> perform the actions upon going to RRC\_IDLE as specified in 5.3.11 with the release cause 'other' upon which the procedure ends;

Références de documentation connexes

Forcer un téléphone portable LTE ciblé dans un réseau d'écoute clandestine

Forcing a Targeted LTE Cellphone into an Eavesdropping Network

chercheur : technologie d'utilisation avancée de la pseudo station de base - briser complètement le code de vérification SMS

[1] CRR LTE : TS 36331

[2] CRR 5G : TS 38331