HOW TO NOT BREAK LTE CRYPTO

VULNÉRABILITÉS AU SEIN DES MODEMS CELLULAIRES ET CONTOURNEMENT DES PROCÉDURES DE SÉCURITÉ LTE

Benoit Michau, Christophe Devine ANSSI

Agence nationale de la sécurité des systèmes d'information

INTRODUCTION

LSF : Laboratoire de sécurité des technologies Sans-Fil
SSTIC 2014 : développement d'un banc de test cellulaire
Evaluer l'implémentation de la norme LTE au sein des modems :

- antenne-relai commerciale (Ettus USRP et Amarisoft eNodeB)
- coeur de réseau sur mesure (corenet)
- ordiphones sous Android

CONSTRUCTEURS DE MODEMS CELLULAIRES

QUALCOMM

- Leader du marché des modems cellulaires (2015 : 65%, ABI Research)
- Modem et processeur applicatif séparés (ex. : Apple A7 + MDM9615M) ou intégrés (ex.: Snapdragon 800 / MSM8974)
- Communication par un lien série sur USB rapide ; protocoles QMI & DIAG, interface IP (wwan)
- Image du modem découpée mais reconstituable ; pas de symboles.

QUALCOMM

- Architecture matérielle basée sur Hexagon ; trois coeurs physiques (DSP cellulaire, DSP audio, proto. cellulaires) avec SMT
- OS temps réel : QuRT/BLAST. SDK Windows/Linux fourni (gcc/LLVM + émulateur et image ELF du DSP audio)
- Pas d'ASLR, mais utilisation de biscuits de pile (matériel depuis Hexagon V61). Documentation des instructions système non publique
- Support dans IDA Pro : module développé par T. Cordier au sein de l'agence, ainsi que https://github.com/gsmk/hexagon

QUALCOMM

- Protocole DIAG tres riche ; non documenté mais implementé dans QXDM (client lourd)
- Remontée de traces réseau complètes ; affichage de messages de déboguage

```
NAS MM/High  emm_security.c 06210 EMM: Invalidating SRVCC CK & IK
NAS MM/High  emm_security.c 06136 EMM: UE received Integrity algo = 0
NAS MM/Error emm_security.c 02536 SMC NAS security algos validation f
NAS MM/High  lte_nas_msg_parse.c 01126 NAS message is not security pr
NAS MM/High  msg_lib_encode_emm.c 00439 Encoding Service reject
NAS MM/High  lte_nas_msg_parse.c 01132 Encoding EMM message
```

- Quelques implémentations open-source (libqcdm, qcombbdbg)

MEDIATEK

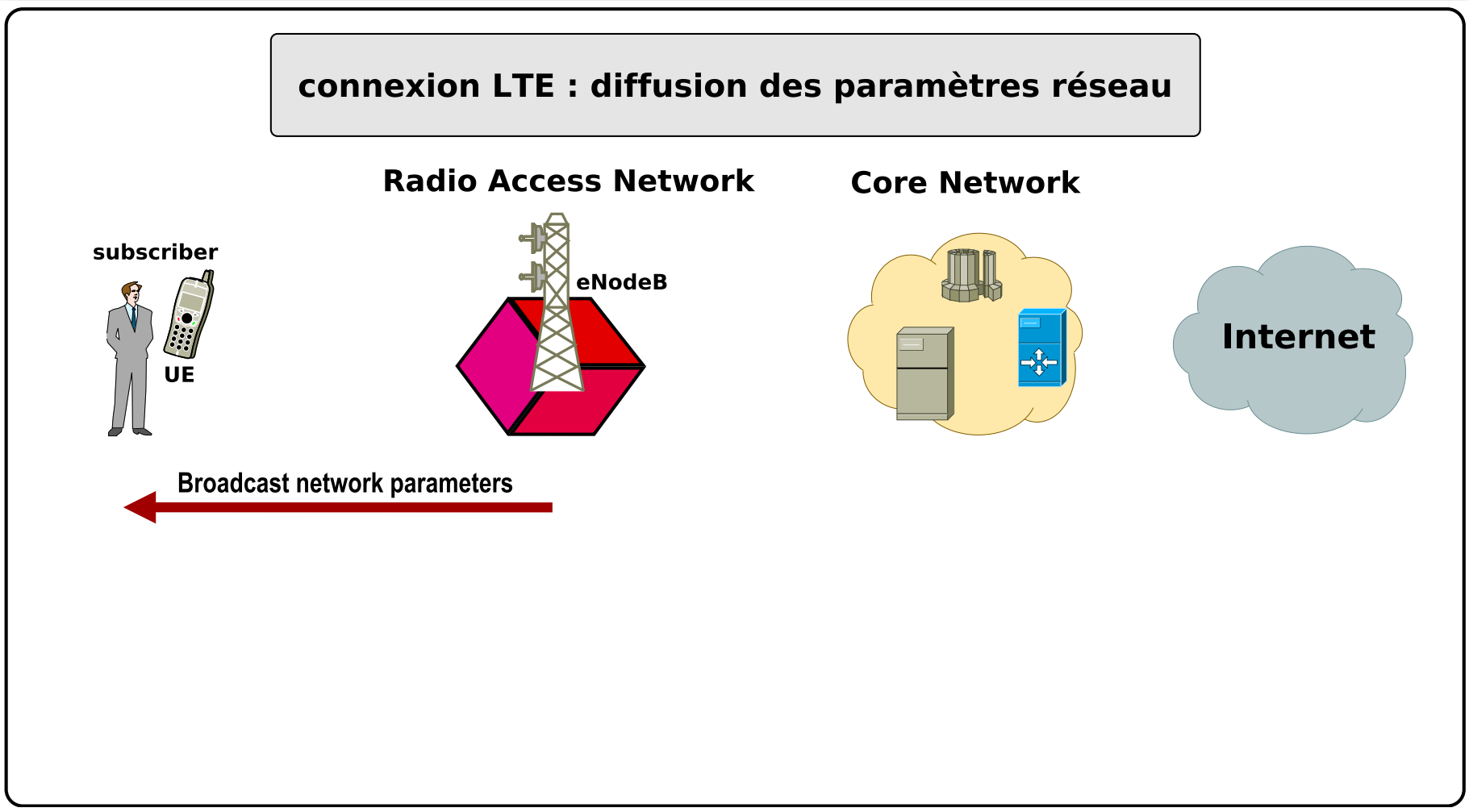
- Téléphones bas/milieu de gamme, souvent double-SIM
- Modem traditionnel (ARM+DSP), gcc 4.6, pas de biscuits de pile/ASLR
- Possibilité d'obtenir des traces de déboguage par l'app. cachée mtklogger
- Fichier présent avec le modem documente les symboles

SAMSUNG

- Produits Samsung uniquement (modem 2G-3G-LTE), Galaxy S6 Corée/Europe
- Firmware du modem obfusqué ou chiffré. Menu *#9900# permet un crash dump en clair de l'image mémoire complète
- Exploité à PACSEC 2015 par N. Golde et D. Komaromy, présentation à venir à RECON 2016.

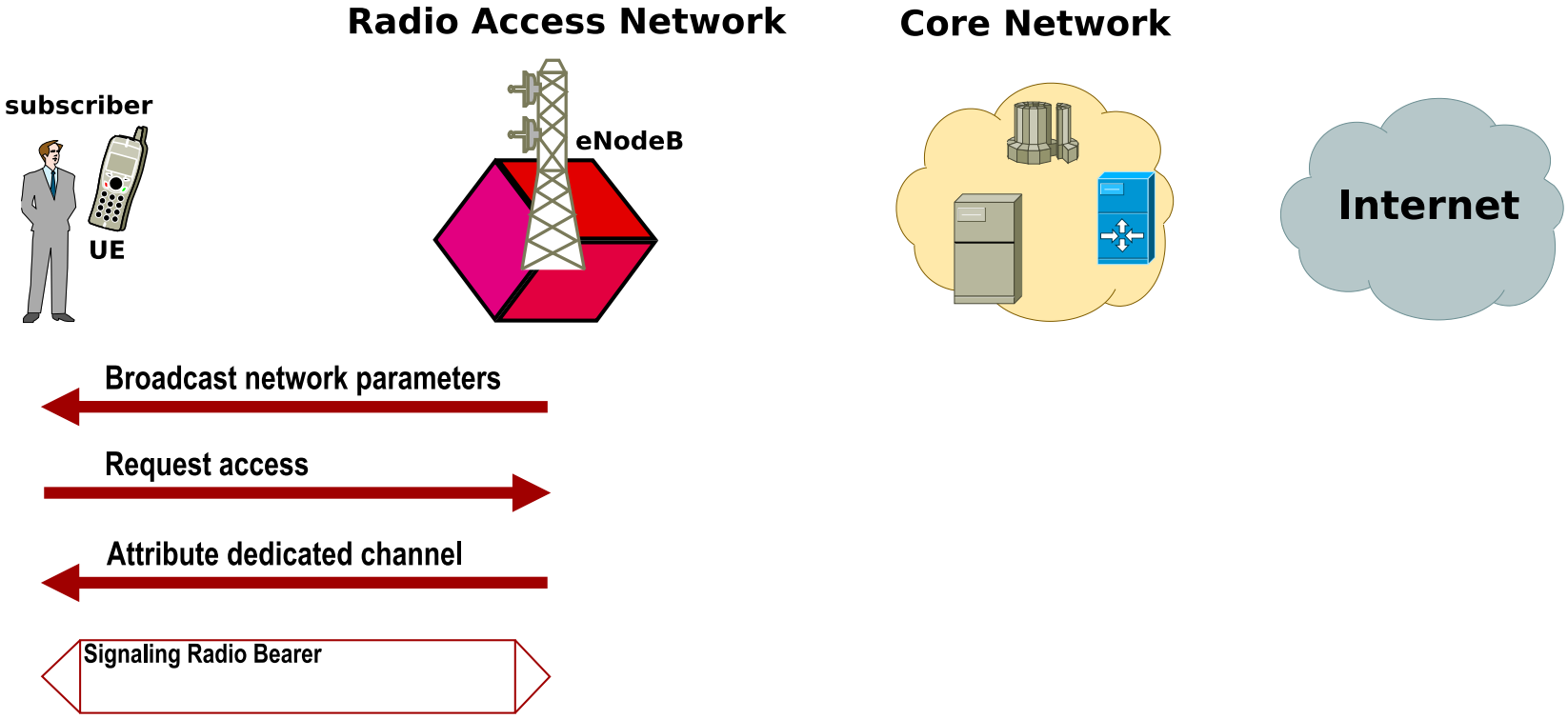
CINÉMATIQUE D'UNE CONNEXION LTE

ETABLISSEMENT DE LA LIAISON RADIO

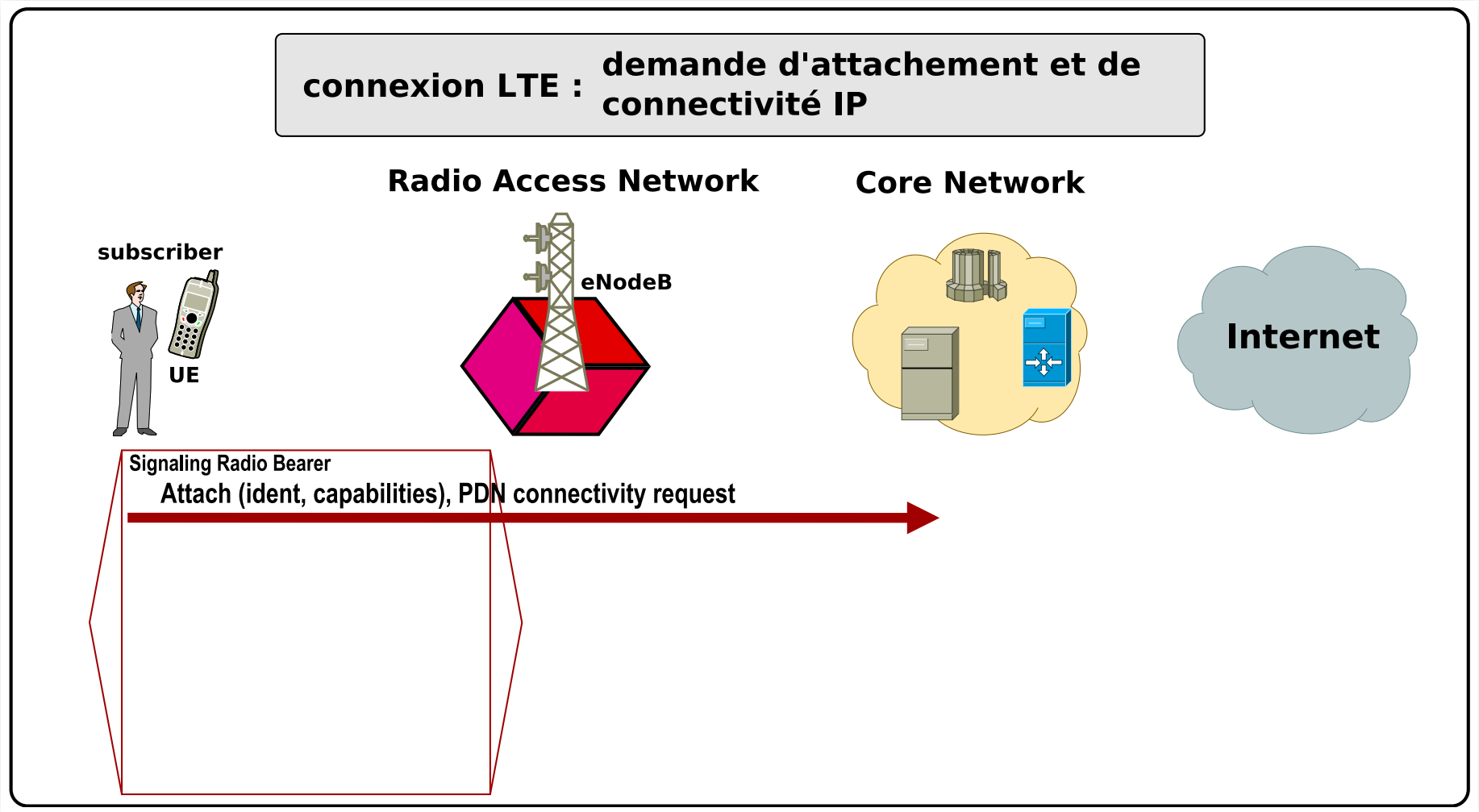


ETABLISSEMENT DE LA LIAISON RADIO

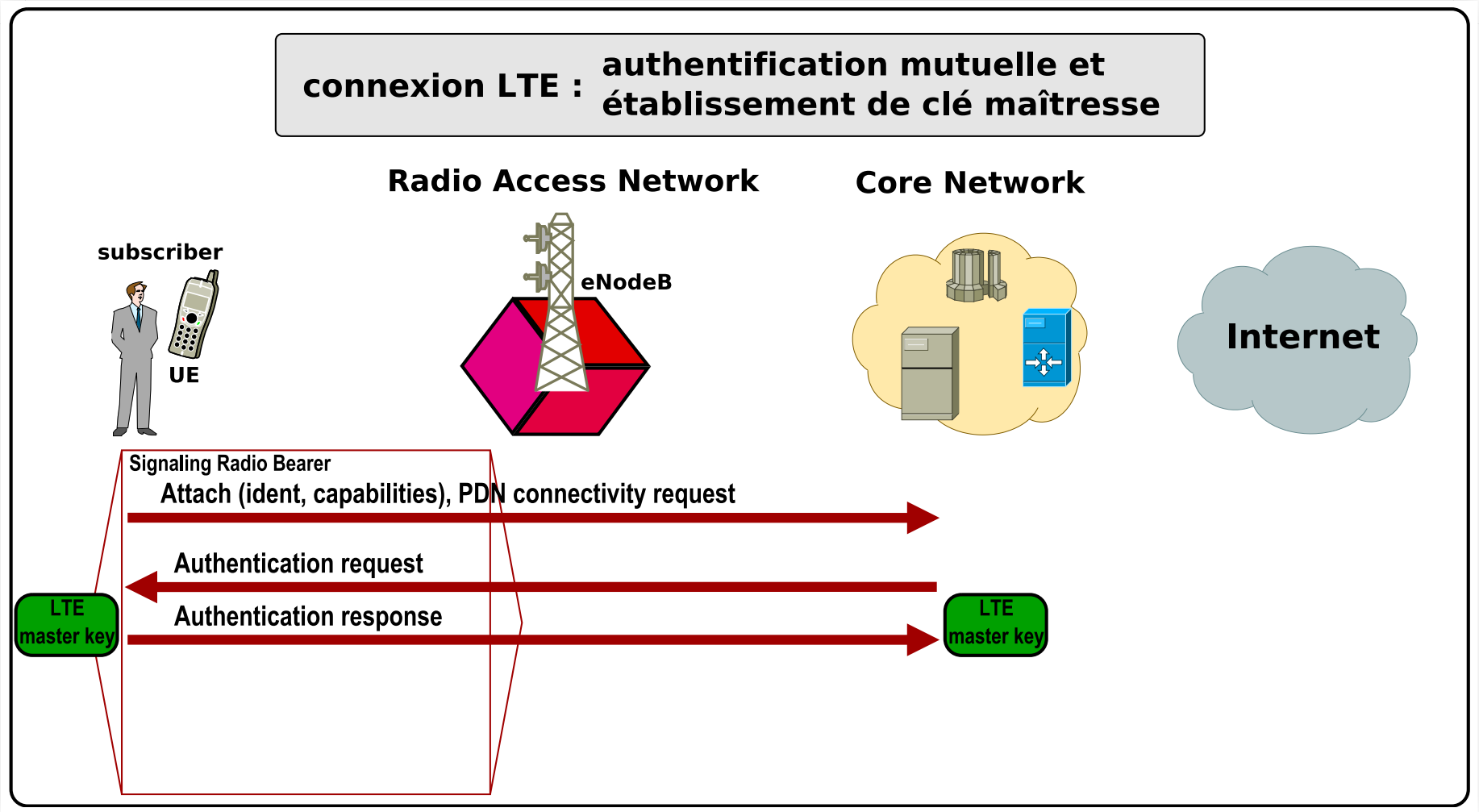
connexion LTE : établissement d'un canal de signalisation dédié



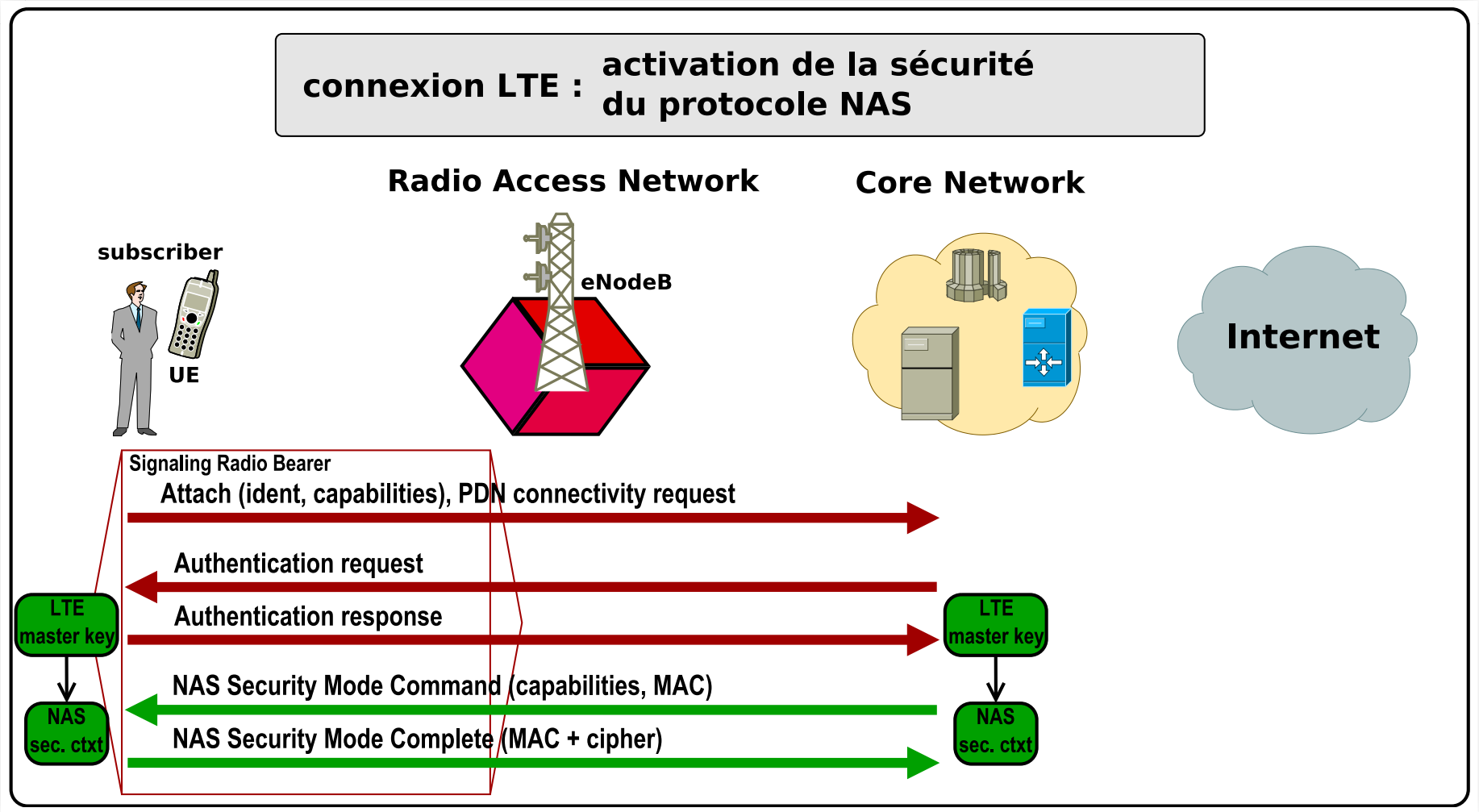
ACTIVATION DE LA SÉCURITÉ NAS



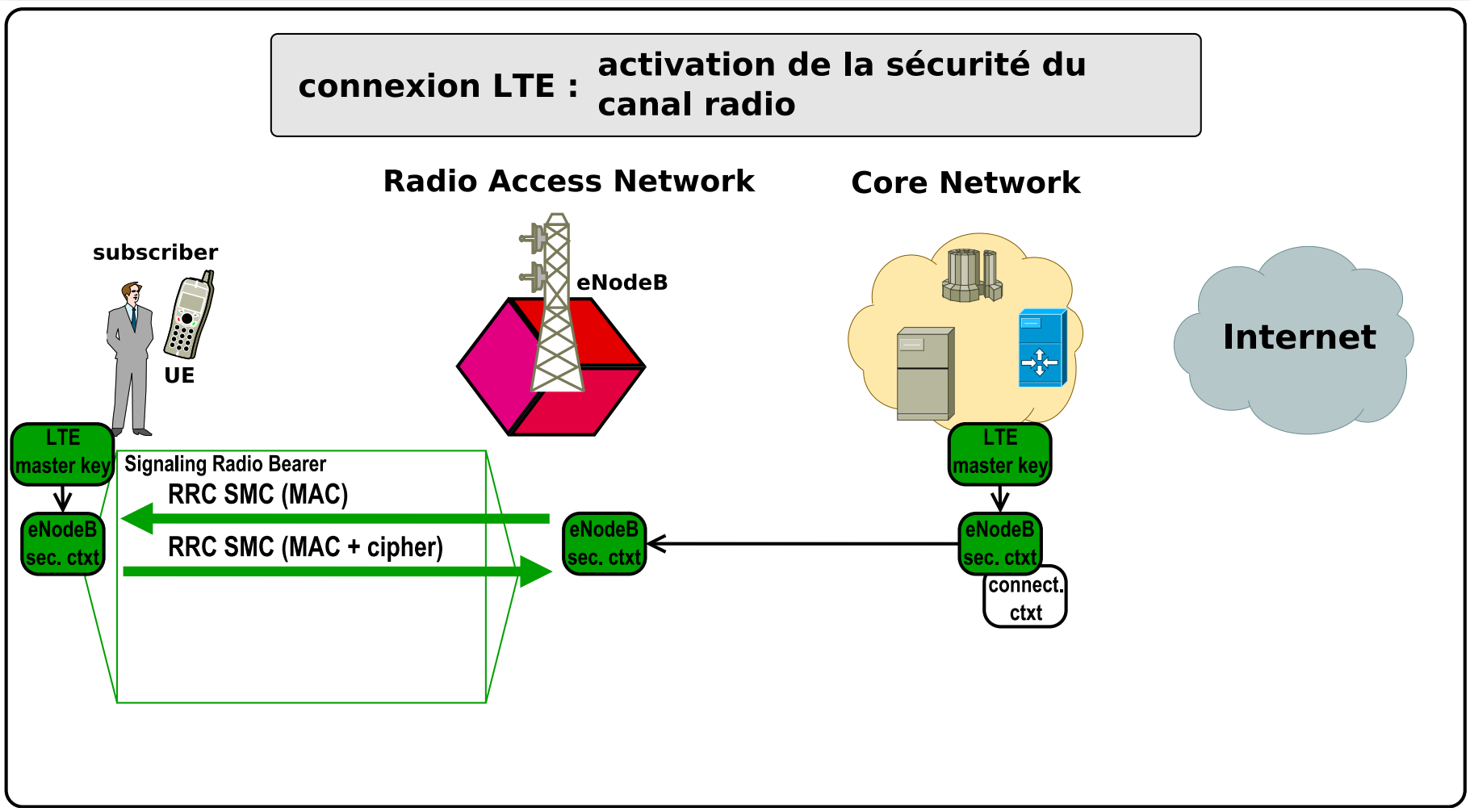
ACTIVATION DE LA SÉCURITÉ NAS



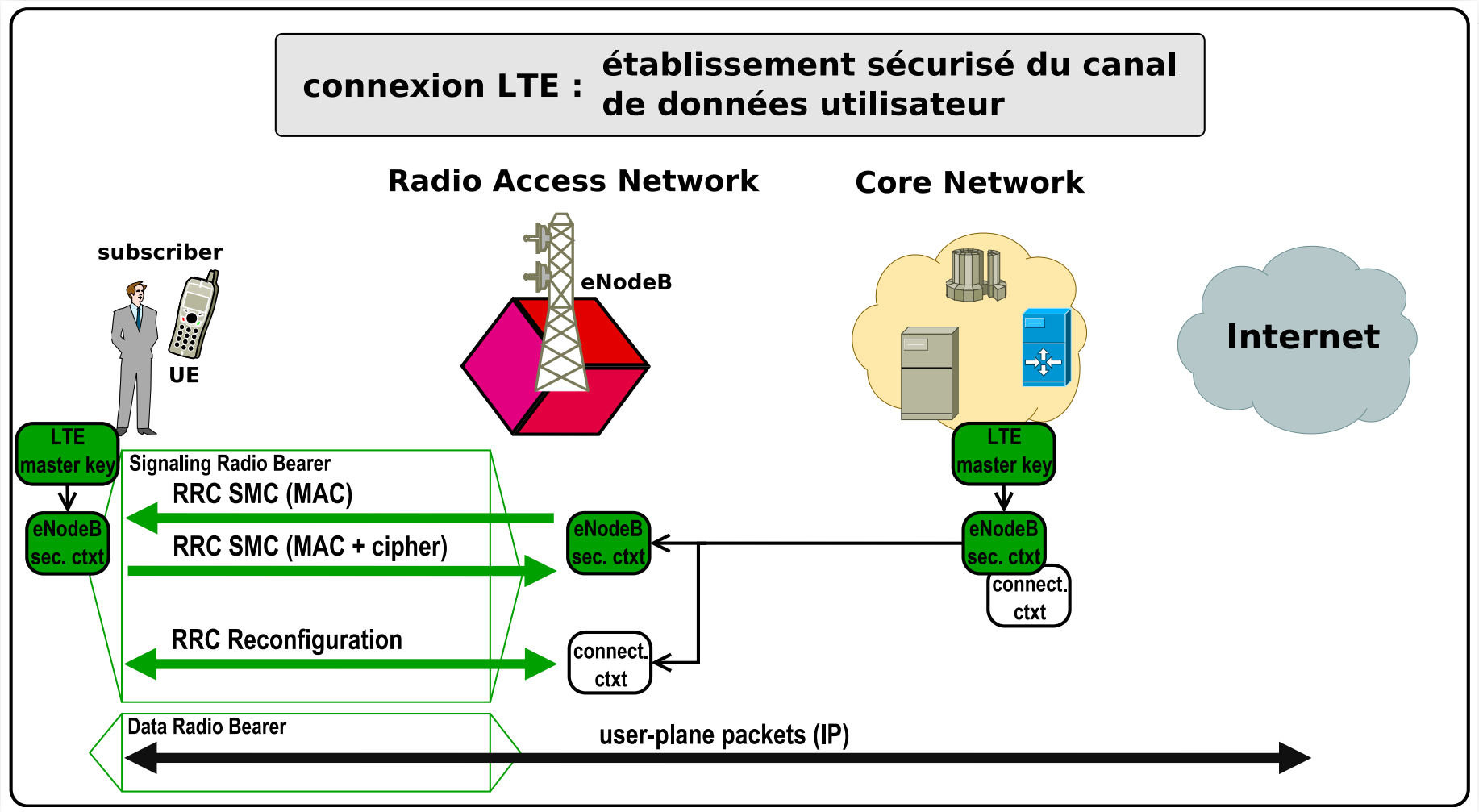
ACTIVATION DE LA SÉCURITÉ NAS



ACTIVATION DE LA SÉCURITÉ RADIO



ACTIVATION DE LA SÉCURITÉ RADIO



EXEMPLES DE VULNÉRABILITÉS

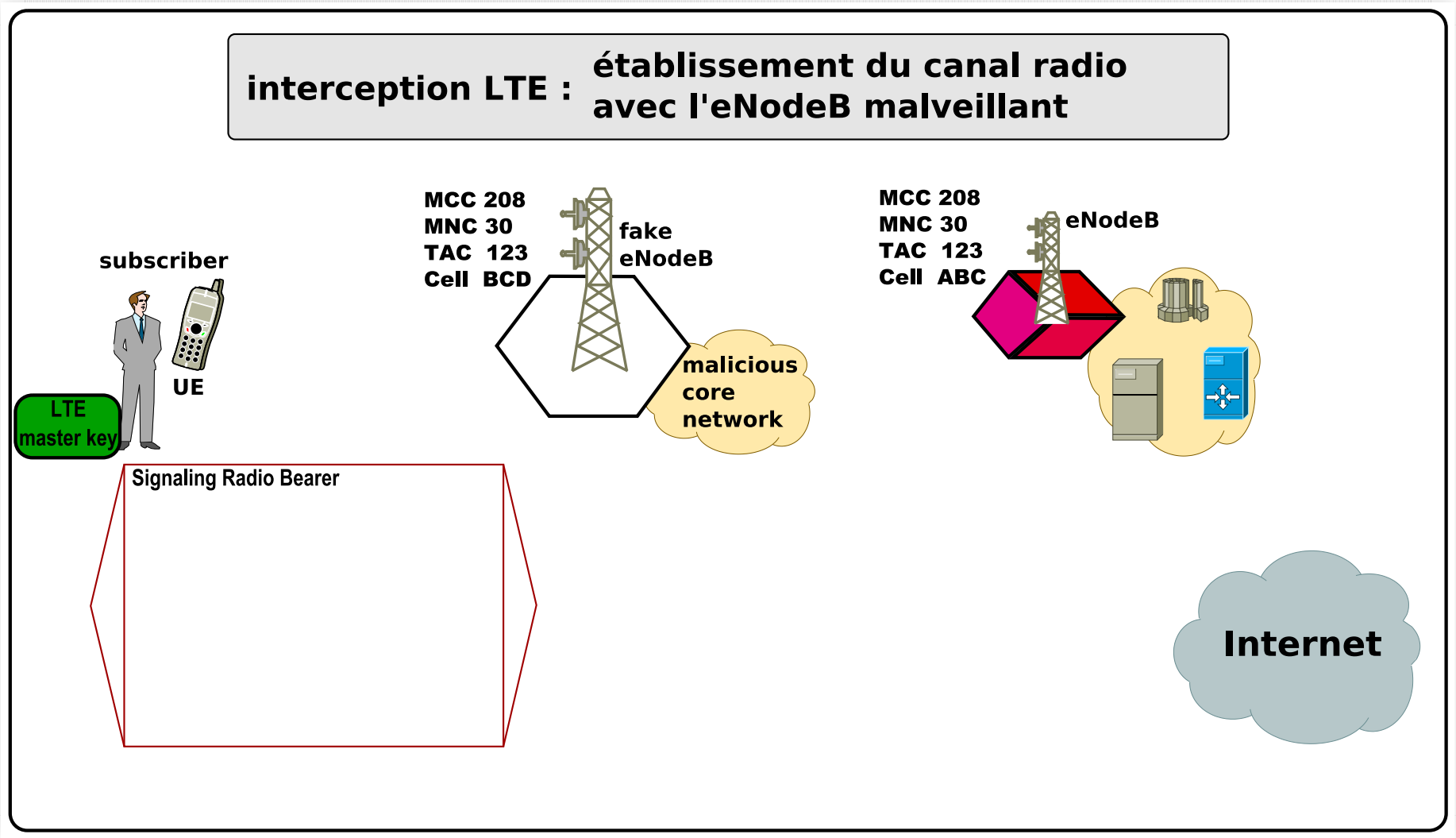
Attaquant actif, capture les abonnés LTE sur une fausse antenne-relai

- proche de la victime (ou signal plus puissant que les antenne-relais environnantes);
- qui usurpe les codes réseaux de l'opérateur de la victime.

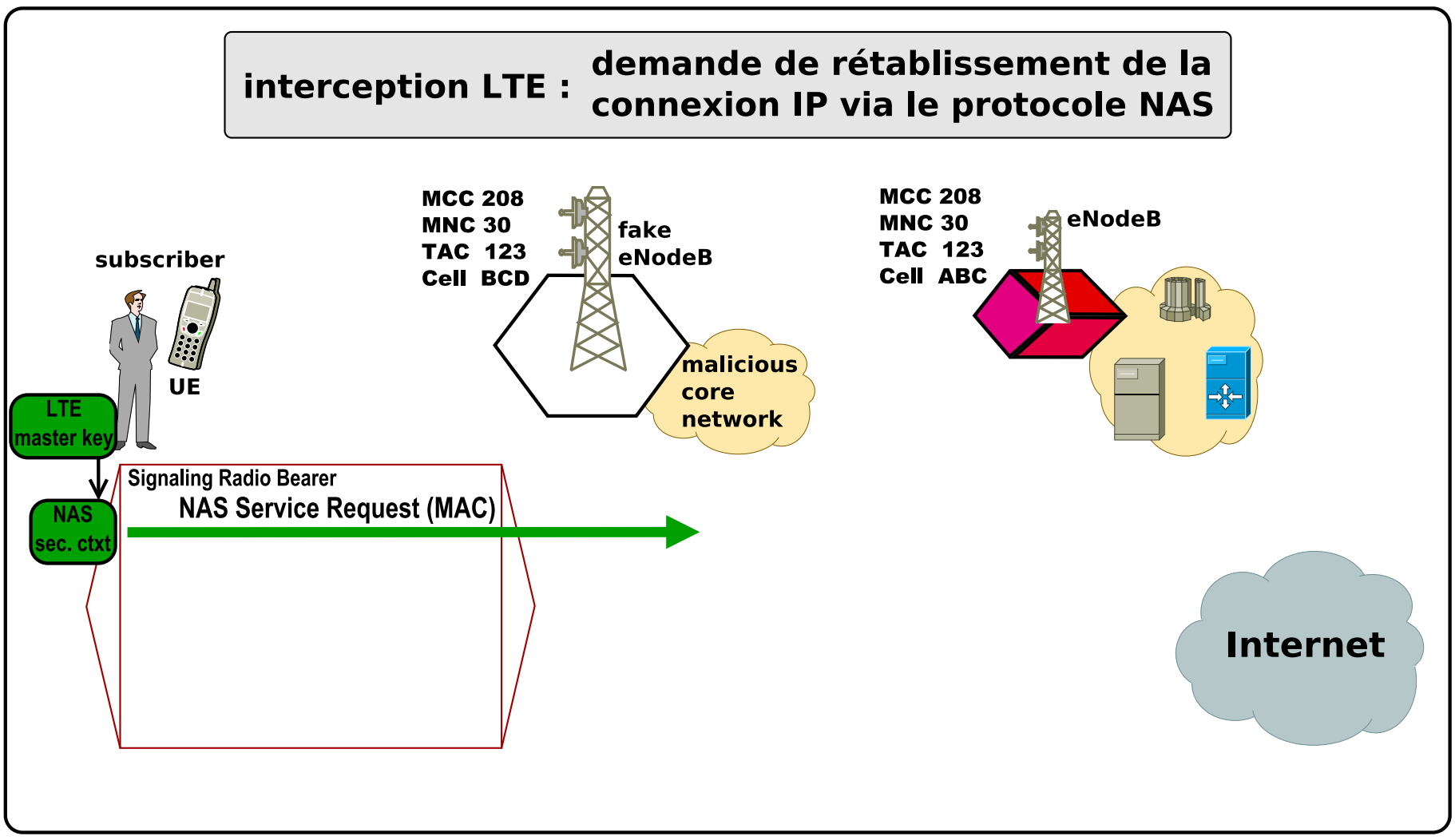
EIA0-RRC

EIA0: contrôle d'intégrité nul, mode interdit pour les connexions LTE normales.
Le modem vulnérable accepte une connexion radio (RRC) sans sécurité (EEA0 et EIA0), mais n'accepte pas EIA0 au niveau NAS.
Permet l'interception du canal de données via une fausse antenne-relai, lors de reconnexions.

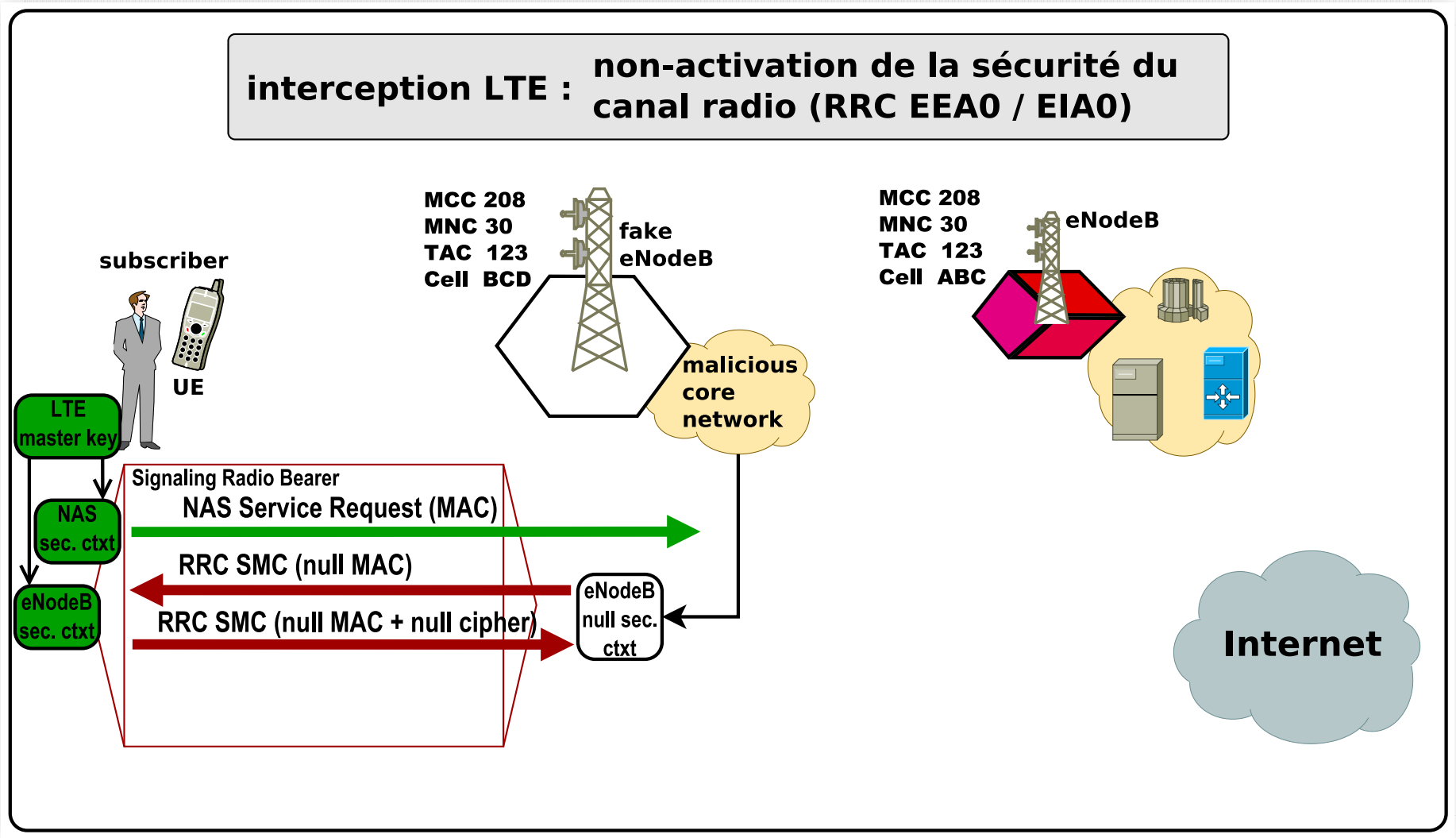
INTERCEPTION LTE AVEC RRC-EIA0



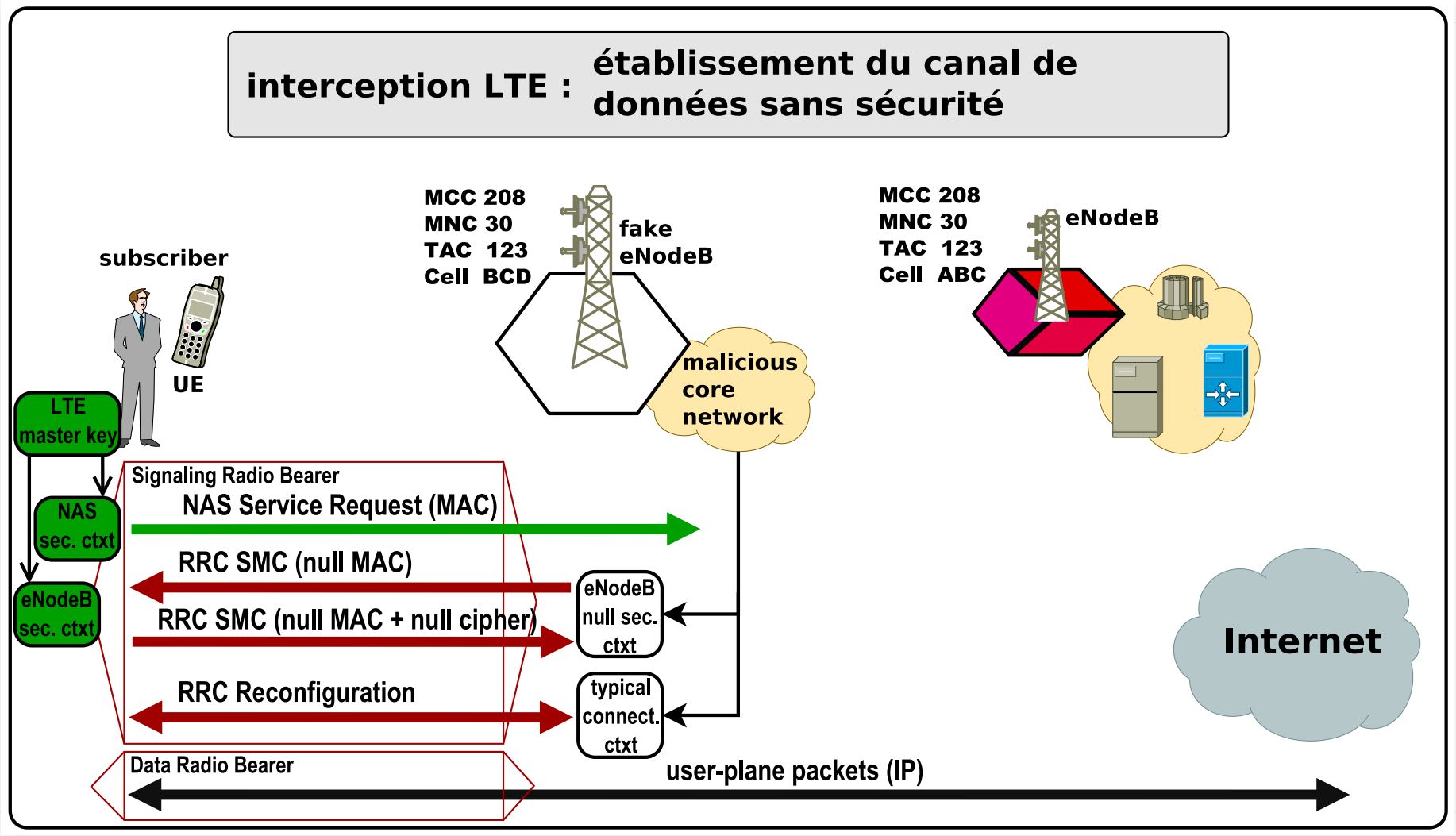
INTERCEPTION LTE AVEC RRC-EIA0



INTERCEPTION LTE AVEC RRC-EIA0



INTERCEPTION LTE AVEC RRC-EIA0



OBTENTION DE PARAMÈTRES ESM SANS SÉCURITÉ

En LTE, tant que la sécurité du protocole NAS n'est pas activée, il est normalement impossible d'obtenir d'autres informations que IMSI et TMSI.
On ne sait jamais, on peut toujours demander ?
esm_info_req.pcap

ESM INFORMATION RESPONSE (DECODÉ PROPREMENT)

```
In [5]: show(parse_L3('0205da28050474657374'.decode('hex')))
### [ESM_INFORMATION_RESPONSE] ###
 <EPS Bearer Type [EBT] : 0>
 <Protocol Discriminator [PD] : '2 : EPS session management messages'
 <Procedure Transaction ID [TI] : 5>
 <[Type] : '218 : ESM information response'>
 ### Access Point Name [APN] ###
  <[T] : 40>
  <[L] : 5>
  <[V] : '\x04test'>
```

OBTENTION DE L'IMEI SANS SÉCURITÉ

En LTE, tant que la sécurité du protocole NAS n'est pas activée, il est normalement impossible d'obtenir d'autres informations que IMSI et TMSI.
Sauf lorsqu'on passe le bit de politesse à 1 !
imei_req.pcap

CONCLUSION

VULNÉRABILITÉS

Les failles de sécurité existent (aussi) dans les modems cellulaires. Tous les modems cellulaires.
Les fabricants les corrigent (losqu'on leur indique). Les failles présentées ici ont toutes été remontées et sont à priori corrigées.
Le déploiement des correctifs jusqu'aux abonnés reste laborieux.

TRANSPARENCE

Aucune.

EVOLUTIONS

Plus de transparence.

Authentification du canal de diffusion des antennes.

Perfect Forward Secrecy.