# La signalisation chez les opérateurs mobiles

Benoit Michau et Marin Moulinier
benoit.michau@p1sec.com
marin.moulinier@p1sec.com

P1 Security

**Résumé.** Dans cet article, nous présentons l'infrastructure réseau d'un opérateur mobile, les différents protocoles de signalisation utilisés, ainsi que les mécanismes de routage entre opérateurs, afin de permettre l'itinérance des abonnés. De nombreux problèmes de sécurité existent du fait de l'exposition des infrastructures entre opérateurs du monde entier, gouvernés par des régulations parfois très différentes. Ces problèmes exposent malheureusement les abonnés (leurs métadonnées : statut, localisation, ainsi que leurs communications) à des tentatives de fraude et d'espionnage, contre lesquelles seuls les opérateurs et les régulateurs peuvent tenter de s'opposer. De plus en plus d'opérateurs installent des équipements de protection, souvent poussés par leur régulateur. Mais le chemin est encore long, et les nouvelles technologies continuent d'arriver en supplément des systèmes existants.

## 1 Introduction

Chez les opérateurs mobiles, le terme « signalisation » est systématiquement utilisé pour indiquer les messages protocolaires échangés entre terminaux et équipements télécoms, qui permettent le fonctionnement des services d'appels et cellulaires. Il s'agit de protocoles spécifiques au monde télécom, qui restent peu connus des utilisateurs de ces réseaux. Et pour cause : il faut soit rooter son smartphone et y installer un outil de diagnostic spécifique au modem (ou baseband), soit travailler chez un opérateur, pour avoir la visibilité sur de tels protocoles.

Mais pourquoi l'accès à ces protocoles est-il si difficile ? Dans le domaine cellulaire, chaque abonné est identifié par un IMSI (*International Mobile Subscriber Identity*), qui l'identifie de manière univoque au niveau mondial. Cet IMSI est inscrit dans la carte SIM de tout abonné cellulaire. Et la plupart des messages de signalisation échangés entre équipements télécoms se rapportent à un abonné spécifique (désigné par son IMSI, ou un identifiant temporaire lié à cet IMSI). Ceci fait de ces messages des données à caractère personnel ! Ce concept est très différent de celui des réseaux fixes, dans lesquels la signalisation s'appuie principalement

sur les adresses IP (DHCP, DNS, BGP...), qui ne sont généralement pas nominatives.

Si on croise cela avec les services rendus par un réseau mobile : localisation, appels et mise en relation d'abonnés, échange de messages courts, connexion à des services de données, nous pouvons comprendre que la signalisation chez les opérateurs télécoms : c'est sensible et ça pique ! Au-delà de cette situation, la régulation nationale (R.226 entre autres) et européenne (RGPD) impose aux opérateurs de protéger correctement ces données personnelles.

Dans la suite de ce document, les points suivants sont abordés :

- l'architecture générale des réseaux mobiles et les protocoles de signalisation qui en sont à la base
- les protocoles de signalisation utilisés au sein de l'infrastructure d'un opérateur
- la manière dont ces protocoles sont utilisés et routés entre opérateurs, pour les besoins de l'itinérance (ou « roaming »)
- les difficultés auxquelles fait face chaque opérateur vis-à-vis de ses partenaires de roaming

Dans cette dernière section, différents aspects sont développés, comme le type d'attaques rencontrées quasi-systématiquement, les moyens de protection et de défense à disposition des opérateurs, des exemples de campagnes d'espionnage et de compromission de données de signalisation, et le rôle des régulateurs pour permettre l'amélioration de la situation.

## 2 Présentation des protocoles

### 2.1 Architecture générale d'un réseau mobile

Les protocoles de signalisation sont variés, selon le segment du réseau dans lequel ils sont utilisés, ainsi que selon la technologie cellulaire. En effet, un réseau mobile est constitué de deux parties distinctes : le réseau d'accès radio (dit RAN pour *Radio Access Network*), et le cœur de réseau (dit aussi *Core Network*). Pour une présentation assez détaillée d'un réseau mobile, de son infrastructure, ainsi que des protocoles mis en œuvre, le lecteur peut se reporter à l'article du SSTIC 2014 sur l'analyse de modems cellulaires [16], ainsi qu'à l'infographie ci-dessous.

De manière grossière, le réseau d'accès radio est constitué par les stations de base, situées au pied des antennes-relais (15 000 à 20 000 pour couvrir le territoire français métropolitain, par exemple), ainsi que des contrôleurs radio en 2G et 3G. Lorsqu'un abonné est connecté à une

antenne-relais, cette dernière peut le localiser avec une précision assez fine, de l'ordre de la centaine de mètres, voire mieux.

Le réseau cœur se décompose, lui, en deux parties distinctes :

- Un « front-end » prenant en charge les services et connexions des abonnés : MSC/VLR et GMSC pour le mode circuit en 2G-3G, SGSN et GGSN pour le mode data en 2G-3G, MME et SGW-PGW pour la 4G ; ce *front-end* maintient à jour la localisation de chaque abonné au niveau d'une plaque géographique couverte par plusieurs antennes-relais (de quelques $km^2$ à quelques centaines de $km^2$).
- Un « back-end » constitué par le HLR en 2G-3G et le HSS en 4G, contenant les profils des abonnés et identifiant le *front-end* par lequel un abonné est pris en charge ; il est complété par un SMS-C (ou *SMS-Center*) qui stocke et fait suivre les SMS des abonnés de l'opérateur vers leur destinataire.

Dans certains scénarios d'itinérance (dits de « home-routing ») et de MVNO, on peut aussi considérer les GGSN et PGW comme étant dans le *back-end* du cœur de réseau.

# Exemple de distribution spatiale des éléments d'un réseau mobile

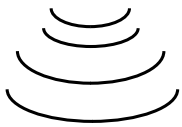
Échelle géographique :

Légende :

Individu

Le terminal utilisateur (mobile, tablette, clef 3G...) est l'extrémité du réseau mobile. Son modem est une puce disposant d'un environnement d'exécution à part, le *baseband*.

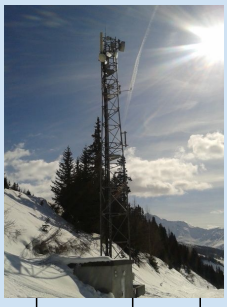
On l'appelle MS (*Mobile Station*), ou ME (*Mobile Equipment*) dans les normes.



L'interface radio utilise une modulation et des bandes qui dépendent parfois du continent/pays, et des protocoles qui dépendent de la technologie d'accès (2G : GSM, 3G: UMTS/HSDPA, 4G : LTE/LTE-A).

Cellule radio

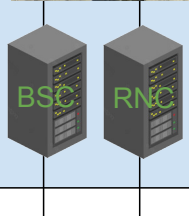
**Partie accès**
(RAN - *Radio Access Network)*



La station de base se trouve à l'extrémité du câble coaxial relié à l'antenne mobile à proprement parler (le *feeder*). Elle traite le signal radio et peut être distribuée en plusieurs modules, par exemple la tête radio (RRU/RRH) plus près du mât et l'unité protocolaire (BBU/RBU) plus loin dans le cas d'un pylône.

- En 2G : BTS (*Base Transceiver Station*)
- En 3G : nodeB, en 4G : eNodeB, etc.

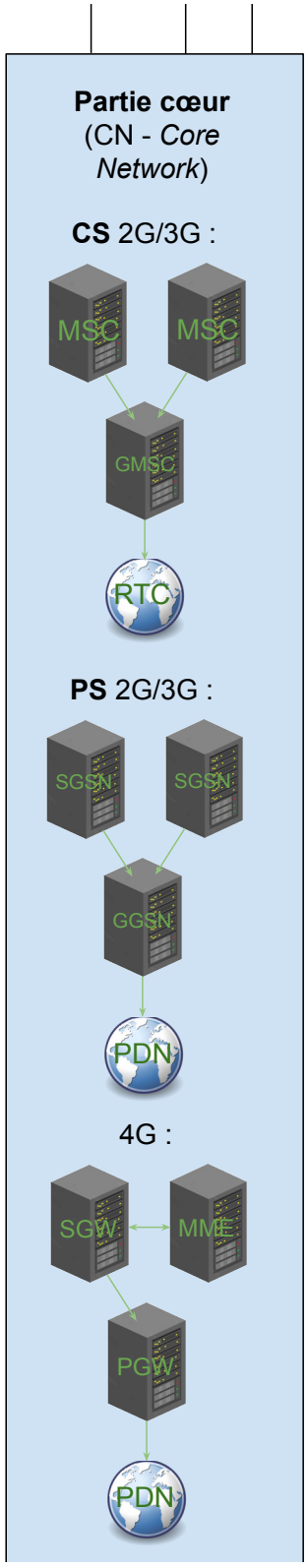
Ville




Le contrôleur logique peut concentrer les flux de plusieurs BTS ou Node B, sur lesquels il effectue un traitement logique.

Il s'appelle BSC (*Base Station Controller*) en 2G, ou RNC (*Radio Network Controller*) en 3G. Il n'existe plus en 4G.

Région




Après leur passage par le réseau d'accès, les flux de signalisation arrivent vers le premier équipement de cœur de réseau, généralement concentré au niveau de la région ou du pays.

En **2G/3G**, cette partie du cœur est découpée en deux domaines différents : le domaine CS (*Circuit-Switched*) qui correspond au cœur 2G d'origine. Et le domaine PS (*Packet-Switched*) qui a été ajouté avec l'arrivée d'Internet sur mobile (la technologie GPRS, 2.5G).

Le mobile s'attache distinctement au CS et au PS. Les appels passent par le CS, le trafic IP passe par le PS et les SMS peuvent passer par l'un des deux (plus souvent par le CS).

Le premier équipement de cœur sur lequel arrive notre trafic de signalisation est donc :

> En **CS**, le MSC (*Mobile Switching Center*) qui est l'équivalent d'un switch pour le réseau mobile, et fait également l'interconnexion avec le réseau téléphonique classique pour les appels [†] [†].

> En **PS**, le SGSN (*Serving GPRS Support Node*) qui est l'équivalent paquet du MSC. Plusieurs SGSN sont reliés à **une passerelle vers Internet**, le GGSN (*Global GGSN Support Node).*

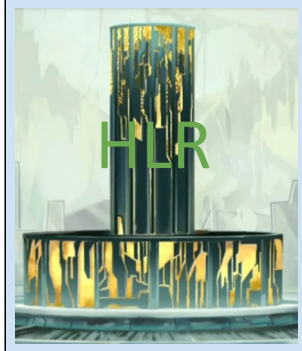
En **4G**, il n'y a plus de séparation CS/PS mais il y a une séparation fonctionnelle :

> Les flux de signalisation pure arrivent vers le MME (*Mobility Management Entity*)

> Tandis que les flux de données (voix ou Internet) arrivent vers le SGW (*Serving Gateway*), et sortent en extrémité par le PGW (*Packet Data Network Gateway*), qui connecte le réseau à IMS ou bien Internet

Le MSC, le SGSN et le MME connaissent la cellule d'attachement de l'abonné sur le réseau, lorsque celui-ci est connecté [†].

Pays






À l'échelle nationale, une seule grande base de données stocke le **profil** de chaque abonné, dont son identifiant unique (**IMSI**), mais aussi et surtout ses **secrets cryptographiques** (dont le **Ki**, clef secrète dupliquée uniquement sur la **carte SIM** de l'abonné*, la téléphonie mobile fonctionnant globalement avec de la **cryptographie à clef partagée** et non de la cryptographie asymétrique).

Cette base de données s'appelle le **HLR** (*Home Location Register*) en 2G/3G et le **HSS** (*Home Subscriber Server*) en 4G.

À l'échelle nationale aussi, on trouve un ou plusieurs SMSC (*Short Message Serving Center*) qui routent les SMS entre les réseaux.

À tous les niveaux du réseau, la signalisation a aussi ses routeurs de niveau 2 : le STP (*Signal Transfer Point*) en SS7, et le DRA (*Diameter Routing Agent*) en Diameter, qui sont susceptibles de s'interfacer entre les équipements du réseau, surtout en bordure d'interconnexion de ce celui-ci.

* À noter que la carte SIM est une carte à puce dotée d'un microcontrôleur, pouvant exécuter des applications natives et JavaCard

† La fonctionnalité de suivi de la cellule des abonnés sur le MSC est appelée VLR (*Visitor Location Register*). Le HLR sait aussi localiser l'abonné, le VLR et le HLR sont des entités séparées afin de permettre le roaming (ils seront sur des réseaux séparés).

†† Un MSC qui s'interconnecte avec le réseau téléphonique commuté (RTC) est appelé GMSC (*Gateway Mobile Switching Center*).

### 2.2 Réseau d'accès radio

Il y a d'un côté les protocoles radio et d'accès :

- entre terminaux et antennes-relais (principalement MAC pour *Media Access Control*, et RRC pour *Radio Resource Configuration*) ;
- entre terminaux et cœur de réseau (dit NAS pour *Non-Access Stratum*, que l'on va considérer ici malgré tout comme un protocole d'accès) ;
- entre antennes-relais voisines ;
- et entre antennes-relais et cœur de réseau.

Dans l'ensemble de ces protocoles, un abonné est identifié soit directement par son IMSI, soit par un identifiant temporaire associé (TMSI pour *Temporary Mobile Subscriber Identity*, RNTI pour *Radio Network Temporary Identifier*). L'opérateur et l'abonné en question ont bien sûr les moyens de faire correspondre ces identités temporaires à l'IMSI. Mais il existe aussi différents moyens pour un attaquant indépendant du réseau de l'opérateur de retrouver la correspondance entre ces identités temporaires et l'IMSI concerné, certains sont décrits dans cette étude [10] de 2017.

Tous ces protocoles sont différents, selon que le terminal et le réseau effectue une connexion 2G, 3G, 4G ou 5G, même s'il existe des similitudes importantes entre certains d'entre eux. La plupart de ces protocoles sont par ailleurs spécifiés avec ASN.1 et utilisent un encodage PER (*Packed Encoding Rules*).

### 2.3 Cœur de réseau

Il y a de l'autre côté les protocoles de cœur de réseau, utilisés entre équipements télécoms, ainsi qu'entre opérateurs :

- SS7 : famille de protocoles de signalisation utilisés dans les cœurs de réseaux 2G-3G ;
- Diameter : protocole utilisé dans les cœurs de réseaux 4G et IMS ;
- GTP : protocole utilisé dans les cœurs de réseaux 2G-3G et 4G pour le contrôle et le transport des sessions de données des abonnés ;
- SBA (en fait HTTP/2) : utilisé dans les cœurs de réseaux 5G, pas encore déployé en cette année 2022.

Avec SS7 comme Diameter, un abonné est identifié par son IMSI (lorsqu'il est pris en charge par le réseau) ou son MSISDN, c'est-à-dire son numéro de téléphone (par exemple lorsqu'il s'agit du destinataire d'une communication). Avec GTP, des identifiants temporaires appelés TEID (pour *Tunnel Endpoint IDentifier*) sont associés à l'IMSI d'un abonné donné puis utilisés. En 5G avec SBA, la notion d'identité d'un abonné est

étendue au-delà du format courant de l'IMSI, nous n'entrerons pas dans ces subtilités cependant.

Enfin, on peut également indiquer l'utilisation des suites de protocoles SIP, SDP et RTP, utilisés par le cœur de réseau IMS (*IP Multimedia Subsystem*). Ce dernier permet d'assurer les services de communications voix (au sens large). L'IMS a été introduit afin de remplacer les services voix nativement supportés par les réseaux 2G-3G en mode circuit (cf section 3.2) ; c'est cette technologie qui est derrière le service VoLTE (*Voice over LTE*). L'IMS est un système autonome et interconnecté au cœur de réseau 4G.

## 3 Usage en interne d'un opérateur

### 3.1 Des acronymes comme s'il en pleuvait

Attention, cette section tente de présenter en détails les protocoles de signalisation les plus utilisés dans les cœurs de réseaux. De très nombreux acronymes sont utilisés, nous ne pouvons malheureusement trop élaborer à propos de chacun d'eux, au risque d'écrire un livre sur le sujet. La compréhension détaillée de ces protocoles n'est pas forcément nécessaire à la compréhension du reste de l'article, et le lecteur ne doit pas s'inquiéter de se sentir un peu perdu à la lecture de cette section.

### 3.2 Signalisation en mode circuit CS en 2G-3G

A l'origine, les réseaux mobiles se sont appuyés sur l'infrastructure des réseaux téléphoniques fixes pour l'établissement des appels en mode circuit, afin de s'intégrer facilement dans l'infrastructure télécom existante des années 80. Le protocole ISUP est ainsi réutilisé entre commutateurs mobiles (MSC/VLR et GMSC) et fixes, afin d'établir et contrôler les appels. De nouveaux protocoles ont été développés pour prendre en charge, entre autres, la localisation des abonnés mobiles et leur authentification : SCCP et TCAP-MAP (IS-41 est une variante de MAP pour les réseaux mobiles nord américains). TCAP-CAP (ou CAMEL) a également été introduit pour gérer la messagerie, le transfert ou renvoi d'appel et d'autres services définis dans le cadre des réseaux dits intelligents (rien à voir avec l'IA cependant, l'IN – pour *Intelligent Network* – date des années 90). On retrouve aussi l'échange des SMS et l'USSD qui sont transportés dans TCAP-MAP. La figure 1 représente permet de visualiser l'organisation de ces protocoles SS7. TCAP, MAP et CAMEL sont définis avec ASN.1 et utilisent l'encodage BER.

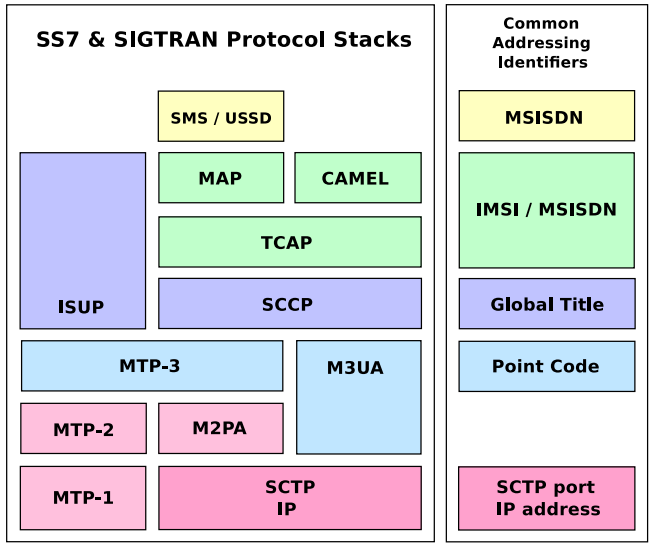



**Fig. 1.** Pile protocolaire SS7

Ces protocoles sont tous transportés à l'origine sur MTP-3 (en mode synchrone), puis sur M3UA (sa variante SIGTRAN pour IP) suite à la migration des réseaux de signalisation du mode circuit vers IP, à partir du début des années 2000. L'ensemble de ces protocoles constitue ce qu'on appelle généralement la famille SS7. Les protocoles MTP, ISUP, SCCP et TCAP sont normalisés par l'ITU-T, alors que MAP, CAP, SMS, USSD sont normalisés à l'origine par l'ETSI, et à présent maintenus par le 3GPP.

Le **tableau 1** qui suit illustre une correspondance informelle entre les différentes couches OSI et les principaux protocoles composant SS7, et en décrit les fonctionnalités.

**Tableau 1.** Les différents protocoles de la *stack* SS7 sont utilisés à de multiples niveaux du réseau 2G-3G, du réseau d'accès radio jusqu'au HLR, et aux interconnexions SMS et voix internationales. À l'origine développée par les opérateurs américains dans les années 1970 et standardisée par le CCITT (ancêtre de l'ITU) dans les années 1980, SS7 couvre tous les aspects du transport de la signalisation jusqu'au niveau 1, avant que le groupe de travail *Signaling Transport* de l'IETF ne définisse une adaptation de SS7 à IP appelée SIGTRAN dans les années 2000.

| | |
|---|---|
| **MTP1** | Il s'agit de la spécification de la couche de **niveau 1** (physique) utilisée pour les liaisons de type SS7 classique. Définie dans la norme ITU-T Q.702, il s'agit à l'origine d'adaptations des normes nord-américaines utilisées pour la transmission longue distance sur liaison cuivre (généralement coaxiale), notamment E1, E2, E3...<br><br>Avec SIGTRAN, elle n'existe plus car le lien physique est remplacé par un transport IP/SCTP, et un ou plusieurs protocoles de la couche SS7 (MTP2, MTP3 et/ou SCCP) sont encapsulés ou réencodés dans un nouveau format TLV plus standard et homogène. |
| **MTP2** | Couche de **niveau 2** (liaison) définie par les normes ITU-T Q.703 et Q.704, comprenant de base des numéros de séquence et une taille. |
| **MTP3** | Première couche de **niveau 3** (réseau) définie par les normes ITU-T Q.703 et Q.704, définissant le principe du **Point code**, l'identifiant réseau de base sur le réseau SS7 (il s'agit en pratique d'une séquence de bits dont la taille et la représentation varient d'un continent à un autre). Tous les équipements SS7 ont un *Point Code*, mais on y a plus tard superposé SCCP (voir ci-dessous) qui est devenu le principal mécanisme de routage de niveau 3 pour les réseaux mobiles. |
| **SCCP** | Seconde couche de **niveau 3** (réseau), définie par les normes ITU-T Q.711 à Q.716. Elle permet notamment le routage par **Global title (GT)**, le principal mécanisme de routage utilisé aujourd'hui sur les réseaux SS7 internationaux. Le GT reprend dans la plupart des cas la syntaxe d'un numéro de téléphone classique. Pour router internationalement un message de signalisation qui concerne un abonné en particulier, on peut aussi mettre un IMSI dans le champ GT (uniquement surles réseaux nord-américains) ou bien un MGT (sorte de mélange entre le préfixe d'un numéro de téléphone classique et le suffixe d'un IMSI). |
| **TCAP** | Couche de **niveau 5** (session) utilisée pour gérer des transactions, une transaction étant une séquence normée de messages applicatifs (MAP, etc.). La transaction TCAP est forcément courte, et est constituée d'une suite elle aussi normée d'états qui dépendent des opérations transportées (requête, réponse, invocation, suite, fin, abandon...). |
| **MAP** | Couche de **niveau 7** (applicatif) utilisée pour toutes les opérations de signalisation liées au cœur de réseau mobile (localisation et profils des abonnés, échange de SMS, etc.). |
| / | Il n'y a pas de couche de niveau 4 (transport) sur le réseau SS7 classique, la règle générale étant qu'un équipement est un *endpoint* protocolaire, et la couche TCAP permettant d'assembler les séquences de messages pour les opérations comprenant plusieurs messages. Sur SIGTRAN, la couche SCTP (niveau 4) transporte l'ensemble de la pile SS7 sur IP. |

### 3.3 Protocoles en mode paquet PS en 2G-3G

Avec l'introduction du GPRS / EDGE et des connexions de données pour les abonnés mobile à la fin des années 90, une nouvelle infrastructure de cœur de réseau est introduite, afin de router les données IP des abonnés. Elle réutilise les protocoles SCCP et TCAP-MAP pour gérer mobilité et authentification, et introduit GTP-U (pour *GPRS Tunneling Protocol - User-Plane*) pour transporter ces paquets IP jusqu'au point de « sortie » du réseau mobile, correspondant à l'APN de connexion de l'abonné. Le protocole GTP-C (pour *GTP - Control-Plane*) est introduit en parallèle afin de gérer l'établissement, la modification et la suppression de ces tunnels GTP-U, au sein de l'infrastructure cellulaire.

Ces protocoles sont normalisés à l'origine par l'ETSI et à présent par le 3GPP. Ils continuent d'évoluer car GTP-C reste utilisé en 4G, et GTP-U en 4G et 5G.

### 3.4 Petit focus sur MAP et les services associés

L'outil « pycrate_map_op_info.py [17] » présent dans la bibliothèque pycrate permet de lister toutes les opérations MAP ou CAMEL, ainsi que leurs arguments détaillés et les équipements impliqués dans une opération TCAP-MAP. En exemple, le listing 1 présente l'opération de relocalisation d'un abonné dans le domaine CS : lorsqu'un abonné se connecte sur un nouveau MSC-VLR, ce dernier contacte le HLR de l'abonné ; le HLR met à jour le contexte de l'abonné avec l'adresse de l'équipement qui le prend en charge, ceci permet à l'abonné de rester joignable.

```
$ pycrate_map_op_info.py -o 2

-------------------------------------------
------  MAP operationCode: (local, 02)  ------
-------------------------------------------

MAP version 3 and over
OPERATION content: ArgumentType - Errors - ResultType -
    operationCode

  ArgumentType: UpdateLocationArg (SEQUENCE)
    - imsi (OCTET STRING)
    - msc-Number (OCTET STRING)
    - vlr-Number (OCTET STRING)
    - lmsi (OCTET STRING)
    - extensionContainer (SEQUENCE)
    - vlr-Capability (SEQUENCE)
    - informPreviousNetworkEntity (NULL)
    - cs-LCS-NotSupportedByUE (NULL)
    - v-gmlc-Address (OCTET STRING)
```

```
20      - add-info (SEQUENCE)
21      - pagingArea (SEQUENCE OF)
22      - skipSubscriberDataUpdate (NULL)
23      - restorationIndicator (NULL)
24      - eplmn-List (SEQUENCE OF)
25      - mme-DiameterAddress (SEQUENCE)
26      mandatory : imsi, msc-Number, vlr-Number
27
28    ResultType: UpdateLocationRes (SEQUENCE)
29      - hlr-Number (OCTET STRING)
30      - extensionContainer (SEQUENCE)
31      - add-Capability (NULL)
32      - pagingArea-Capability (NULL)
33      mandatory : hlr-Number
34
35
36  MAP version 1 and 2
37  OPERATION content: ArgumentType - Errors - ResultType -
        operationCode
38
39    ArgumentType: UpdateLocationArg (SEQUENCE)
40      - imsi (OCTET STRING)
41      - locationInfo (CHOICE)
42      - vlr-Number (OCTET STRING)
43      - lmsi (OCTET STRING)
44      mandatory : imsi, locationInfo, vlr-Number
45
46    ResultType: UpdateLocationRes (CHOICE)
47      - hlr-Number (OCTET STRING)
48      - extensibleUpdateLocationRes (SEQUENCE)
49
50
51  Initiator in MAP application context:
52    - networkLocUpContext-v3                    (0 4 0 0 1 0 1 3)
53      {vlr} -> {hlr}
54    - networkLocUpContext-v2                    (0 4 0 0 1 0 1 2)
55      {vlr} -> {hlr}
56    - networkLocUpContext-v1                    (0 4 0 0 1 0 1 1)
57      {vlr} -> {hlr}
```

**Listing 1.** paramètres de l'opération de relocalisation en CS

### 3.5 Signalisation Diameter

Le développement de la 4G à la fin des années 2000 a entrainé un renouvellement d'une partie des protocoles de signalisation par Diameter, protocole normalisé à l'origine par l'IETF pour succéder à RADIUS. Il est introduit dans les réseaux mobiles, et grandement étendu afin de prendre en charge les mécanismes de localisation et d'authentification au sein des cœurs de réseaux 4G, ainsi que bien d'autres fonctionnalités annexes.

De fait, Diameter remplace MTP-3/SCCP/TCAP-MAP et CAMEL, en fournissant des services à peu près équivalents. Cela aurait pu donner

lieu à une grande simplification, cependant la structure des messages Diameter utilisés dans les réseaux mobiles a malheureusement conservé une complexité importante, doublée d'un léger laxisme inhérent aux protocoles IETF.

### 3.6 Usage intra-opérateur

L'ensemble de ces protocoles permettent de réaliser un très grand nombre d'opérations distinctes entre les différents équipements d'un cœur de réseau mobile, et systématiquement vis-à-vis d'un abonné spécifique. Chaque opérateur opère ses réseaux de manière cohérente (tout du moins est-on en droit de l'espérer). Ainsi le fait d'exposer des interfaces permettant de connaître ou contrôler des informations précises, en termes de localisation ou de services en cours d'utilisation, pour chaque abonné ne pose pas de gros problèmes de sécurité, tant que ces interfaces sont cloisonnées à l'intérieur d'un domaine de sécurité bien identifié chez chaque opérateur.

Ce problème de cloisonnement des interfaces se pose malheureusement depuis de nombreuses années, avec l'avènement de l'itinérance et l'installation de passerelles et de routeurs entre les opérateurs du monde entier.

## 4 Utilisation de la signalisation entre opérateurs

### 4.1 Principes de l'itinérance

Le principe de l'itinérance consiste à permettre à tout abonné mobile ayant souscrit un forfait auprès d'un opérateur national, une prise en charge par un opérateur dans un autre pays. Pour ce faire, les deux opérateurs impliqués doivent permettre la connexion entre le « front-end » du cœur de réseau du VPLMN (*Visited Public Land Mobile Network*, le réseau qui prend en charge la connexion de l'abonné) et le « back-end » du cœur de réseau du HPLMN (*Home PLMN*, le réseau d'origine de l'opérateur de l'abonné, qui dispose entre autre de son profil et génère ses données d'authentification).

Ceci implique, pour un opérateur donné :

- que son « front-end » (ses MSC/VLR et SGSN en 2G-3G, MME et SGW en 4G, tout au moins) soit accessible au « back-end » de tous ses partenaires de roaming, ceci afin de prendre en charge des abonnés venant de l'étranger sur son réseau ;

- et que son « back-end » (ses HLR, HSS et SMS-C tout au moins) soit accessible au « front-end » de tous ses partenaires de roaming, afin de permettre à ses abonnés d'être pris en charge à l'étranger.

Ces deux principes sont très simples, leurs implications d'un point de vue technique sont cependant très importantes. L'infrastructure de chaque opérateur doit, de ce fait, être exposée auprès de centaines d'autres opérateurs tout autour du monde !

## 4.2 Interconnexions et routage

Pour un opérateur, établir des interconnexions avec quelques partenaires de roaming demeure faisable ; mais lorsqu'il s'agit de centaines de réseaux à l'étranger, chacun s'appuyant sur des fournisseurs éventuellement différents, avec des configurations spécifiques, la situation devient moins facile à gérer. À ce jour, 197 états sont reconnus par l'ONU dans le monde, plus de 750 opérateurs sont inscrits à la GSMA [20], et près de 3 000 codes d'opérateurs mobiles sont renseignés dans Wikipédia [21].

Les opérateurs ont ainsi mis en place, via la GSMA, l'association mondiale des opérateurs GSM, un système de déclaration d'itinérance, s'appuyant sur une fiche dite IR.21 (*Internal Recommendation n° 21*). Chaque opérateur y liste ses préfixes de numérotation, ses codes réseaux, ses adresses IP, certaines configurations (par exemple concernant le support de VoLTE). Cela facilite la mise en œuvre des interconnexions entre opérateurs, qui s'appuient essentiellement sur les informations mises à disposition dans ces IR.21, via l'application RAEX [1]. Celle-ci est accessible via Internet lorsqu'on dispose d'un compte sur l'infocentre de la GSMA, et est opérée par l'entreprise Roamsys-next [2]. Chaque opérateur (pour chaque pays) y est identifié par un TADIG (code à 5 caractères, commençant par le code pays ; par exemple *FRAF3* pour Bouygues Telecom), et y renseigne un formulaire qui est ensuite converti et mis à disposition sous format PDF et XML aux autres opérateurs.

**Fournisseurs d'interconnexions**

Face à l'accroissement du nombre d'opérateurs mobiles dans le monde, et aux difficultés pour réaliser des interconnexions fonctionnelles en grand nombre, des entreprises au rayonnement continental, voire international, mais peu connues du public, se sont constituées. Ces fournisseurs d'interconnexions, également appelés fournisseurs de services GRX / IPX (pour *GPRS Roaming eXchange* et *IP eXchange*) permettent de réaliser le routage de la signalisation entre opérateurs, en évitant à chaque opérateur

de configurer des règles de routage spécifique à chacun de ses partenaires de roaming.

Ainsi, lorsqu'un VPLMN prend en charge un abonné étranger, ce VPLMN envoie les messages de signalisation concernant cet abonné vers son fournisseur d'interconnexion. Ce dernier, en accédant au contenu du message, détermine le HPLMN de l'abonné, et route le message vers le « back-end » de ce réseau (comme illustré dans la figure 2). Ces fournisseurs peuvent également effectuer dans certains cas des modifications des messages de signalisation, afin d'éviter certaines incompatibilités ou dysfonctionnements empêchant une bonne prise en charge des abonnés en itinérance.

Ces fournisseurs d'interconnexions sont connectés entre eux dans la plupart des cas. Ceci fait qu'un opérateur, en établissant un contrat avec un ou deux fournisseurs, pourra proposer des services d'itinérance sur la quasi-totalité du globe, sans avoir à établir des centaines d'interconnexions directes avec d'autres opérateurs. Parmi les fournisseurs de roaming les plus connus, on trouve Syniverse, BICS (filliale de Belgacom), Arelion (anciennement TeliaCarrier), iBASIS, Comfone, SAP... Certains gros opérateurs disposent également d'interconnexions qu'ils commercialisent souvent sous la dénomination *Wholesale* ou *Carrier* : Orange, Deutsche Telekom, Vodafone, Telefonica, A1 Telekom Austria, Tata Communications... La plupart de ces entreprises, ou activités, ne sont généralement pas exposées au grand public, et revêtent ainsi une opacité importante. Seul le fournisseur AMS-IX publie des statistiques de traffic [5] issues de son hub d'interconnexions à Amsterdam.

Aujourd'hui, la plupart de ces interconnexions sont réalisées via des VPN IPsec sur Internet, entre opérateurs et fournisseurs d'interconnexions.

**Routage en SS7 avec SCCP**

En SS7, la signalisation échangée entre opérateurs est routée par des STP (*Signaling Transfert Point*), qui sont installés au sein et en bordure des réseaux mobiles 2G-3G. Un message de signalisation SS7 entre deux opérateurs peut passer par de multiples STP, certains appartenant à des fournisseurs d'interconnexion tiers. Chaque STP va disposer d'adresse(s) IP pour fonctionner sur les réseaux IP, et d'un SPC (*Signaling Point Code*), l'identifiant au niveau MTP-3. L'ITU-T maintient une liste de SPC internationaux (ou ISPC), dont une version complète est disponible au sein du bulletin opérationnel 1199 [11]. Il faut noter que les SPC sont

également utilisés pour identifier les équipements et STP des réseaux de téléphonie fixe fonctionnant en mode circuit.

Dans le cas des réseaux mobiles, les GT (pour *Global Title*), adresses utilisées au sein du protocole SCCP, identifient les équipements terminaux : source et destination d'un message de signalisation. Un GT est similaire à un MSISDN, sauf qu'il identifie non pas un abonné, mais un équipement télécom. Pour vulgariser au maximum, lorsqu'un STP route un message SS7, il identifie le GT de destination dans le message, détermine le pays (via le préfixe de numérotation) et l'opérateur auquel il appartient (généralement via une configuration statique constituée, entre autres, à partir des fiches IR.21 des opérateurs), et détermine le STP auquel faire suivre le message (son adresse IP et son SPC). De nombreux autres mécanismes de routage existent, s'appuyant sur les SPC et GT, mais aussi les identifiants E.214 (MGT) et E.212 (IMSI), qui peuvent également prendre place au sein du champ GT. Nous n'entrerons cependant pas dans ces détails.

La figure 2 donne un exemple d'interconnexion fictive entre trois opérateurs 2G-3G, via un ou deux fournisseurs d'IPX/GRX.

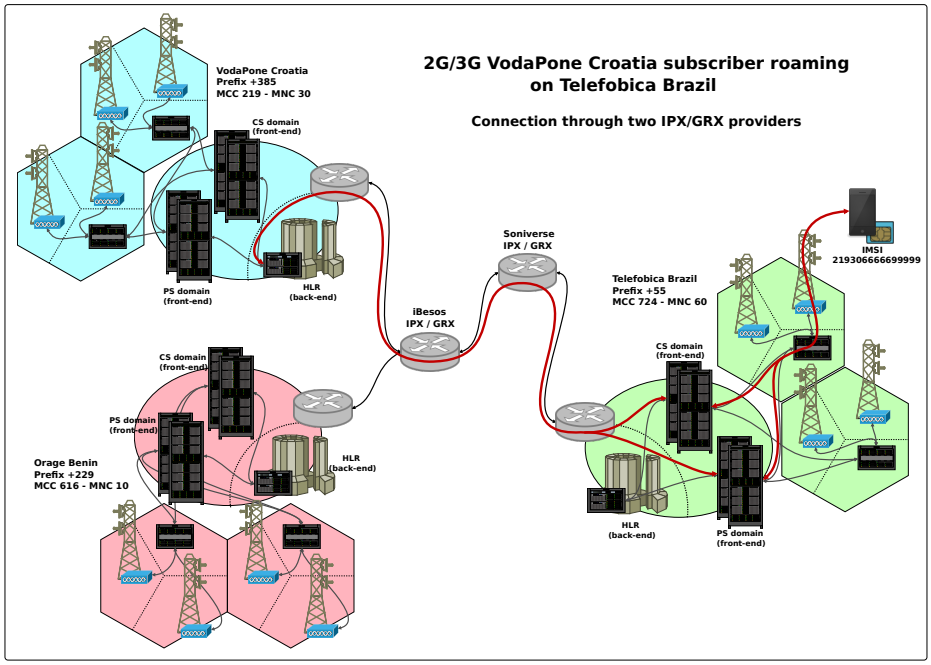



**Fig. 2.** Exemple d'interconnexions 2G-3G IPX/GRX

**Routage avec Diameter**

En 4G, avec le protocole Diameter, la signalisation entre opérateurs est routée par des DRA (*Diameter Routing Agent*), qui sont installés au sein et en bordure des réseaux mobiles 4G. Lorsqu'un DRA est en bordure d'un réseau, on peut également l'appeler DEA (*Diameter Edge Agent*). De même qu'en SS7, un message de signalisation Diameter peut passer par de multiples DRA, dont ceux de fournisseurs d'interconnexion tiers. Chaque DRA dispose d'adresse(s) IP, et les opérateurs mobiles s'identifient avec leurs *realm* (ou domaines), souvent de la forme *mnc123.mcc234.3gppnetwork.org*, qui sont inclus dans chaque message Diameter. Cette construction s'appuie sur les codes réseaux alloués à chaque opérateur (par exemple le code MCC 208 pour la France, et le code MNC 01 – ou 001 en Diameter – pour Orange). Ainsi, en fonction du *realm* de destination indiqué dans un message Diameter, le DRA choisit l'adresse IP du DRA (ou équipement) suivant vers lequel router le message.

Il est étonnant de s'appuyer sur des adresses (ou *realm*) de source et de destination qui sont inscrites dans les messages à router, mais c'est ainsi que Diameter est utilisé dans les réseaux 4G. On peut indiquer qu'en sus du *realm*, le *host* de la source et de la destination (correspondant généralement au nom d'hôte complet de la machine) sont éventuellement présents dans les messages entre opérateurs. Le routage de la signalisation 4G en Diameter, c'est un peu comme si on mettait les adresses IP dans les payloads TCP ! Cette situation permet malheureusement des scénarios de *spoofing* relativement variés dès lors qu'on s'adresse à un DRA qui ne contrôle pas la cohérence des adresses IP sources avec les *realm* d'origine dans les messages. Et cela arrive régulièrement...

## 5 Sécurité sur les interconnexions inter-opérateurs

### 5.1 Difficultés de contrôle de l'opérateur sur ses abonnés

Cette section a pour but d'illustrer le type d'attaque classique que l'on retrouve sur les réseaux de signalisation internationaux, tout en insistant sur la difficulté que peuvent avoir les opérateurs à s'en protéger.

**Correspondance entre MSISDN et IMSI**

Lorsqu'un opérateur indélicat souhaite obtenir des informations sur un abonné mobile, il doit au préalable disposer de son IMSI. Au départ, celui-ci ne dispose souvent que de son numéro de téléphone (MSISDN), et doit par conséquent le « résoudre » en IMSI. Plusieurs procédures de

signalisation existent en SS7 comme en Diameter, permettant d'obtenir l'IMSI à partir d'un MSISDN. La plupart de ces procédures sont filtrées sur les interconnexions internationales, selon les recommandations de la GSMA, mais la procédure de routage des SMS, dite « Send-Routing-Info-for-SM » (ou SRISM), qui est nécessaire au fonctionnement des SMS à l'international, permet une telle résolution. Les opérateurs ont cependant les moyens de se protéger contre cette résolution de MSISDN en IMSI, en installant un *SMS Home-Router* (ou SMS-HR). Se reporter à la section 5.3 pour des détails concernant ce système.

De nombreux opérateurs continuent malheureusement de fonctionner sans SMS-HR, ou avec un équipement mal configuré. Par ailleurs, la richesse des protocoles de signalisation en termes de procédures, de messages et d'encodages, va souvent bénéficier à l'attaquant pour tenter de contourner les mécanismes de défense mis en œuvre par un opérateur ciblé. Dès lors que l'attaquant obtient l'IMSI d'un abonné cellulaire, il va pouvoir effectuer des tentatives pour collecter des informations sur ce dernier, et éventuellement intercepter certaines de ses communications.

**Obtention de la localisation**

Le principe même de fonctionnement d'un réseau mobile consiste à connaitre la localisation des abonnés, afin que ceux-ci puissent être joints à tout moment. C'est aussi souvent la donnée recherchée par les attaquants. Différents équipements dans un cœur de réseau mobile mémorisent la localisation des abonnés avec différents degrés de précision. Il existe également des procédures entraînant une connexion vers l'abonné pour une mesure précise de la position de ce dernier, permettant ultimement d'obtenir sa position GPS.

De même que pour limiter la possibilité d'obtenir la correspondance entre MSISDN et IMSI, la GSMA recommande le filtrage de certains messages et procédures entre opérateurs à l'international. Mais une fois de plus, la richesse des protocoles de signalisation va servir l'attaquant qui va tenter d'obtenir la position d'abonnés ciblés, avec la plus grande précision possible, et éventuellement de manière régulière afin de pouvoir tracer ses déplacements.

**Contrôle de localisation des abonnés**

Un abonné mobile n'est pas connecté en permanence à une antenne-relais, mais uniquement lorsque son terminal a besoin d'échanger des données (ou de prendre en charge un appel). Lorsque le terminal n'est pas connecté à une antenne-relais, il reste « à l'écoute » de celle-ci, au cas où il serait

notifié, par exemple pour la réception d'un appel ou d'un SMS. Dans ce cas, on dit du terminal qu'il est en mode IDLE. Ce faisant, un opérateur n'est assuré de la localisation d'un abonné que lorsque ce dernier est connecté directement à son réseau. Mais dès lors qu'il repasse en mode IDLE, le réseau ne conserve que la dernière localisation active de l'abonné.

Que se passe-t-il, alors, lorsque le *front-end* d'un réseau étranger indique au *back-end* du réseau d'origine d'un abonné, que cet abonné est relocalisé à l'étranger ? Le réseau d'origine n'a d'autre possibilité que de faire confiance au réseau étranger car aucune procédure cryptographique ne permet d'authentifier la présence de l'abonné dans ce réseau étranger. Cela change quelque peu en 5G, nous n'entrerons cependant pas dans les détails ici : le lecteur assidu pourra se reporter à l'article [3] publié dans le MISC 115. Cela reste totalement d'actualité en 2G, 3G et 4G.

Imaginons qu'un opérateur étranger peu scrupuleux décide de relocaliser un abonné cible sur son infrastructure (afin de se placer par exemple en interception de ses appels et SMS, voir la section suivante à ce sujet), le réseau d'origine ne dispose pas de moyens techniques sûrs afin d'éviter cette situation, ou de refuser cette relocalisation. Les guides techniques éditées par le GSMA pour la sécurité de l'itinérance proposent aux opérateurs d'évaluer la faisabilité réelle des relocalisations en fonction des distances géographiques et durée entre les procédures, au sein de pare-feu de signalisation. Autant dire qu'un tel type de filtrage est relativement délicat !

On peut tout à fait imaginer qu'il se passe quelque chose de bizarre lorsqu'un abonné (ou tout du moins son IMSI) fait du ping-pong entre les USA et Israël, ou entre l'Allemagne et la Chine. Mais comment discriminer de telles relocalisations « sauvages » si elles ont lieu entre réseaux frontaliers ? Ou avec un opérateur « international » (comme un opérateur satellite) ? A l'inverse, une relocalisation vers un réseau qui semble lointain, mais pouvant disposer d'antennes-relais à bord de bateaux par exemple, doit-elle être considérée comme illégitime et rejetée ?

Il s'agit ici d'une difficulté majeure concernant l'analyse de la localisation des abonnés mobiles, et par conséquence, de la sécurité des communications associées.

**Interception des communications**

Comment le *front-end* d'un réseau étranger peut-il se placer en interception des communications d'un abonné en le relocalisant chez lui ?

Il faut au préalable que l'opérateur indélicat trouve le *front-end* (MSC/VLR, SGSN/GGSN, MME/SGW/PGW) légitime, en charge de l'IMSI ciblé. Ceci n'est pas forcément évident car les guides techniques de la GSMA proposent également des règles de filtrage empêchant les partenaires de roaming d'obtenir de telles informations, lorsque l'abonné ciblé est sur son réseau d'origine. Ce type de filtrage n'est cependant pas toujours évident à mettre en œuvre, étant donné la complexité des procédures de signalisation, et les multiples mécanismes de routage permis. Certains opérateurs n'ont même parfois aucun mécanisme de filtrage en place...

Dès lors que l'attaquant arrive à obtenir les adresses des équipements réellement en charge, il va pouvoir indiquer au *back-end* du réseau d'origine de l'abonné (le HLR / HSS) que celui-ci s'est déplacé sur son réseau, puis rediriger les communications vers le *front-end* réellement en charge afin que les communications de l'abonné continuent d'être routées de bout en bout. Ce type de scénario est assez simple à mettre en place pour les SMS, plus complexe pour les communications vocales et de données, mais tout de même réalisables. Des conflits peuvent aussi se produire lors de certains types de communications. Il s'agit ici juste d'expliquer le principe de base des interceptions via les interconnexions de roaming ; de très nombreuses variantes existent, selon le type de services ciblés (SMS, USSD, appels, boîte vocale, connexions de données, MMS...).

## 5.2 Services illégaux

La valeur intrinsèque des données gérées par chaque opérateur mobile a nourri la mise en place de services à l'éthique douteuse, visant justement à permettre la résolution de MSISDN en IMSI et l'obtention d'informations techniques sur des IMSI spécifiques (localisation, adresses des équipements qui les prennent en charge...). De tels types de services sont généralement dénommés « HLR lookup » car ils consistent souvent au départ à requêter les HLR (ou HSS) de l'opérateur de l'abonné ciblé. Une simple recherche sur Internet permet de réaliser que de tels services existent en nombre, et peuvent être utilisés par quiconque moyennant finance (de l'ordre du centime d'euro par lookup pour obtenir des informations basiques). Certains ne servent cependant qu'à vérifier l'attachement d'un terminal au réseau à des fins marketing (par exemple pour la réalisation de campagne d'envois de SMS), et non à obtenir des données personnelles.

Ces services fonctionnent sous couvert que les utilisateurs s'engagent sur l'honneur à ne requêter que des numéros qui leurs appartiennent. Les opérateurs de ces services quelques peu hostiles disposent également d'installations techniques dans des pays qui n'ont généralement pas une régulation des télécoms très restrictive, et s'associent à des opérateurs ou fournisseurs d'interconnexions IPX / GRX qui souhaitent faire du business sans s'encombrer de questions éthiques ! On retrouve ainsi ces opérateurs peu scrupuleux installés dans de petits pays, souvent insulaires. On peut citer Jersey, Guernesey, Malte, Chypre, certaines îles des Caraïbes, certains petits pays d'Afrique ou d'Asie ; le fait est que les attaquants n'ont pas de difficulté à trouver un pays où s'installer dès lors que leur activité est suffisamment lucrative !

L'avènement de services internationaux pour l'envoi de SMS en masse, au service des petites et grandes enseignes commerciales du monde entier, a également poussé les opérateurs télécoms et d'infrastructure de réseaux mobiles à s'ouvrir encore plus à des fournisseurs tiers. De nombreuses entreprises proposent ainsi l'envoi de SMS par milliers, avec une couverture continentale voire mondiale. De fait, ces entreprises ont accès aux réseaux de signalisation internationaux, en particulier SS7. Récemment, l'entreprise *Mitto AG*, basée en Suisse, a été dénoncée comme utilisant son infrastructure de distribution de SMS et d'accès aux réseaux de signalisation SS7 à des fins d'espionnage [9].

### 5.3 Moyens de protection pour les opérateurs

De multiples moyens de défense existent pour que les opérateurs protègent leur infrastructure et leurs abonnés des malversations commises par certains de leurs partenaires de roaming (qui, dès lors, portent bien mal leur nom de « partenaire »).

Tout d'abord la mise en place d'un filtrage basique afin d'éviter tout simplement la prise en charge de certaines procédures par le *back-end* et le *front-end* du cœur de réseau. Certains STP SS7 et DRA Diameter permettent la mise en place de tels filtres statiques. Les équipements terminaux eux-mêmes peuvent également permettre de configurer les seules procédures autorisées (ou interdites) en fonction de l'adresse source.

Ensuite, la mise en place d'un SMS Home-Router, afin d'éviter de révéler les IMSI réels de ses abonnés à partir de leur MSISDN. Ceci permet par ailleurs à l'opérateur d'analyser l'ensemble des SMS à destination de ses abonnés, y compris lorsque ceux-ci sont en itinérance à l'étranger. Il est vrai qu'en France, les opérateurs ne sont à priori pas en droit

d'accéder aux contenus des communications, mais certains mécanismes de filtrage peuvent être mis en place sur les en-têtes de SMS, ou un hash du contenu, afin de détecter des problèmes de spam ou phishing SMS, ou des tentatives de compromission de terminaux ou de cartes SIM.

Enfin, un pare-feu de signalisation complet devrait également être installé, afin d'effectuer un filtrage contextuel de la signalisation provenant des réseaux exterieurs, comme expliqué dans la section 5.1. Ce type de pare-feu permet de filter la signalisation SS7 et Diameter en s'appuyant sur le contexte de chaque abonné (entre autres, sa localisation). Il permet également de filtrer le protocole GTP-C afin de s'assurer qu'il n'y ait pas de tentatives de détournement des connexions de données, lorsque celles-ci sont routées entre opérateur à l'étranger et opérateur d'origine (ce procédé est aussi appelé *home-routing* des connexions de données).

D'un côté, depuis une dizaine d'années, les opérateurs mettent de plus en plus en œuvre ce type de mesures de sécurité. Grâce à cela, les guides techniques et équipements gagnent en maturité, d'un point de vue fonctionnel. D'un autre côté, ces équipements peuvent régulièrement souffrir de défauts d'implémentation, du fait de fonctions toujours plus complexes. Les attaquants savent tirer profit de ces défauts pour contourner les politiques de sécurité établies par les opérateurs. Ainsi, aucun moyen de protection ne semble ultime et incontournable, et il convient également d'effectuer une surveillance des interconnexions, via des outils de supervision de la sécurité au niveau télécom.

### 5.4 Compromissions et espionnage

Dans le monde feutré des opérateurs mobiles et télécoms, rares sont les incidents qui donnent lieu à de longs articles dans la presse généraliste. Globalement, seules des interruptions de services majeures sont relayées, telles que le problème ayant touché le service de numéro d'urgence [4] en France en juin 2021. De fait, les attaquants sur les réseaux télécoms réalisent sans doute des bénéfices plus durables et substantiels lorsque leurs actions n'entrainent pas de telles interruptions.

Certaines entreprises de sécurité et certains médias s'attardent heureusement régulièrement sur des cas d'espionnages, et permettent de prendre conscience un tant soit peu, de la manière dont les attaquants opèrent. On peut citer quelques cas récents :

- Le média Vice a mis en lumière [15] l'opérateur d'interconnexions Syniverse, dont l'infrastructure permet l'interconnexion d'opéra-

teurs du monde entier pour l'Amérique, et est apparemment restée compromise entre 2016 et 2021.
- Crowdstrike a publié en 2021 un rapport [12] expliquant la compromission d'opérateurs mobiles via leurs serveurs eDNS (les DNS utilisés pour résoudre, entre autre, les APN et permettre le routage des connexions de données en itinérance) et l'exfiltration de données.
- Un article [6] de CitizenLab de 2020 décrit le mode opératoire de la société Circle, effectuant des malversations sur les réseaux SS7 ; société probablement affiliée à NSO Group, qui a distribué ces dernières années des malwares ciblant principalement iPhone et terminaux Android.
- Le média The Guardian explique [19] en 2020 comment les méchants chinois espionnent les gentils américains depuis des infrastructures de fournisseurs chinois, installées chez des opérateurs mobiles de la zone caraïbéenne.
- Un autre article [8] décrit l'usage de systèmes de signalisation mobiles pour des campagnes d'espionnage, à partir des îles anglo-normandes.
- Mandiant a également publié un rapport [18] en 2019 sur la compromission de SMS-Center d'opérateurs mobiles.
- Adaptive Mobile décrit dans un blogpost [7] détaillé, et peu avant l'entrée en guerre de la Russie en Ukraine, comment certaines campagnes d'espionnage SS7 d'origine Russe seraient camouflées au sein du routage international.

L'ensemble de ces articles semblent parfaitement serieux, et les procédés techniques décrits tout à fait réalistes.

### 5.5 Difficultés des régulations nationales

Les équipements de sécurité et de filtrage restent souvent coûteux, car complexes, comme la plupart des équipements télécoms. Tous les opérateurs ne peuvent ou ne souhaitent pas en installer : après tout, le fait que les abonnés d'un opérateur puissent être espionnés n'engendre bien souvent pas (ou peu) de pertes financières à l'opérateur. Par conséquent, c'est souvent aux régulateurs de pousser (voire de forcer) les opérateurs à déployer des mesures de défense.

À l'échelle mondiale, encore de nombreux opérateurs sont peu, voire pas du tout protégés, au niveau de leurs interconnexions de roaming. En France, et plus largement en Europe, la régulation des télécoms est assez stricte et pousse les opérateurs à mettre en œuvre de telles défenses. En

Amérique du Nord, les régulateurs tentent de pousser les opérateurs à plus de sécurité ; malheureusement, le marché y est tellement ouvert du point de vue commercial, que les données des abonnés américains sont loin d'être les mieux protégées. Cela est visible lorsqu'on regarde de plus près la commercialisation des données de localisation [13] ou la manière dont les SMS sont distribués [14].

Enfin, les régulateurs fonctionnent tous au niveau national, et n'ont quasiment aucune emprise sur les activités agressives d'opérateurs au-delà de leurs frontières.

## 6 Conclusion

Lorsqu'un attaquant cible une entreprise privée, il cible généralement le patrimoine immatériel de l'entreprise (la propriété intellectuelle, les contrats, clients et prospects...), qui incluent éventuellement des données personnelles : nom, email, parfois numéro de tel, numéro de carte bancaire... Dans le cas d'un opérateur mobile, le patrimoine de l'entreprise est constitué principalement des données personnelles de ses abonnés : nom, adresse, identifiant de compte en banque, numéro de télephone, IMSI, localisation au cours du temps, SMS échangés, interlocuteurs et durée des appels, connexions de données, résolutions DNS, contenus des communications... pour des millions d'habitants d'un pays. Un tel niveau de détails de données personnelles n'existe à priori nulle part ailleurs (sauf peut-être à la NSA) !

Les attaquants qui ciblent les opérateurs mobiles ont conscience de cette valeur, et font en sorte de pérenniser leurs activités en restant discrets. Il y a très peu d'actes de « délinquance » informatique sur les infrastructures cellulaires, qui restent assez robustes et redondantes par ailleurs. Un intérêt d'effectuer du renseignement via les réseaux de signalisation mobiles est également qu'il ne laisse quasiment aucune trace sur les terminaux des abonnés, contrairement à l'installation de malware. Enfin, les opérateurs sont souvent peu enclins à empêcher et/ou surveiller leurs interconnexions de signalisation, car ces faits d'espionnage n'impliquent la plupart du temps aucune perte financière pour eux. Ainsi, c'est bien souvent aux régulateurs d'imposer la mise en place de moyens de défense, qui demeurent parfois perfectibles ou faillibles.

Au final, des efforts restent à faire globalement, afin que les opérateurs mettent en place des moyens de défense et de protection efficaces au bénéfice de leurs abonnés. Du point de vue de l'abonné, malheureusement

aucun moyen technique ne permet de se protéger puisque les données de signalisation le concernant sont entièrement gérées par son opérateur. Seule reste la possibilité de protéger le contenu de ses communications avec des systèmes de messagerie et d'appels sécurisés, tels que Signal.

## 7 Remerciements

Merci à Aurélien Roose pour sa relecture et ses précieuses remarques, à toutes les équipes P1 Security pour leur support et la bonne humeur générale, ainsi qu'au comités d'organisation et de programme du SSTIC pour leur travail de grande qualité.

## Références

1. RoamsysNext Login. `https://login.raextools.com/`.
2. RoamsysNext – Driving global connectivity. `https://roamsys-next.com/`.
3. La sécurité des communications 5G. May 2021.
4. Évaluation de la gestion par l'opérateur Orange de la panne du 2 juin et de ses conséquences sur l'accès aux services d'urgence. July 2021. `https://www.economie.gouv.fr/files/2021-07/Rapport-Orange-SNU.PDF`.
5. AMS-IX Amsterdam. Mobile traffic AMS. `https://www.ams-ix.net/ams/documentation/mobile-traffic-ams`.
6. Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, Ron Deibert. Running in Circles Uncovering the Clients of Cyberespionage Firm Circles. *The Citizen Lab - University of Toronto*, December 2020. `https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/`.
7. Cathal McDaid. The Hunt for HiddenArt. *Adaptive Mobile*, February 2022. `https://blog.adaptivemobile.com/the-hunt-for-hiddenart`.
8. Crofton Black. Spy companies using Channel Islands to track phones around the world. *The Bureau of Investigate Journalism*, December 2020. `https://www.thebureauinvestigates.com/stories/2020-12-16/spy-companies-using-channel-islands-to-track-phones-around-the-world`.
9. Crofton Black, Ryan Gallagher. Swiss tech company boss accused of selling mobile network access for spying. *The Bureau of Investigate Journalism*, December 2021. `https://www.thebureauinvestigates.com/stories/2021-12-06/swiss-tech-company-boss-accused-of-selling-mobile-network-access-for-spying`.
10. Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Yongdae Kim. Location Leaks on the GSM Air Interface. *NDSS Symposium*, 2012. `https://syssec.kaist.ac.kr/~yongdaek/doc/fookune_ndss_gsm.pdf`.
11. ITU-T. ITU Operational Bulletin No. 1199. June 2020. `https://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-OB.1199-2020-OAS-PDF-E.pdf`.

12. Jamie Harries, Dan Mayer. LightBasin : A Roaming Threat to Telecommunications Companies. *CrowdStrike*, October 2021. https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/.
13. Jon Keegan, Alfred Ng. There's a Multibillion-Dollar Market for Your Phone's Location Data. *The Markup*, July 2021. https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.
14. Joseph Cox. A Hacker Got All My Texts for $16. *Vice*, March 2021. https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber.
15. Lorenzo Franceschi-Bicchierai. Company That Routes Billions of Text Messages Quietly Says It Was Hacked. *Vice*, October 2021. https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked.
16. Benoit Michau. Analyse de sécurité des modems mobiles. *SSTIC*, 2014. https://www.sstic.org/media/SSTIC2014/SSTIC-actes/Analyse_securite_modems_mobiles/SSTIC2014-Article-Analyse_securite_modems_mobiles-michau.pdf.
17. Pycrate project. "pycrate/tools/pycrate_map_op_info.py" - Github. https://github.com/P1sec/pycrate/blob/master/tools/pycrate_map_op_info.py.
18. Raymond Leong, Dan Perez, Tyler Dean. MESSAGETAP : Who's Reading Your Text Messages ? *Mandiant*, August 2019. https://www.mandiant.com/resources/messagetap-who-is-reading-your-text-messages.
19. Stephanie Kirchgaessner. Revealed : China suspected of spying on Americans via Caribbean phone networks. *The Guardian*, December 2020. https://www.theguardian.com/us-news/2020/dec/15/revealed-china-suspected-of-spying-on-americans-via-caribbean-phone-networks.
20. Tim Hatt, Peter Jarich. Global Mobile Trends 2021 - Navigating Covid-19 and beyond. *GSMA Intelligence*, December 2020. https://data.gsmaintelligence.com/api-web/v2/research-file-download?file=141220-Global-Mobile-Trends.pdf&id=58621970.
21. Wikipedia. List of mobile operators. https://en.wikipedia.org/wiki/List_of_mobile_network_operators.