Sécurité d'un réseau mobile et responsabilité de l'opérateur

Pascal Nourry
pascal.nourry@orange.com

Orange S.A.

Résumé. Usuellement, les articles se focalisent sur la sécurité des interfaces radio ou la sécurité des interfaces de signalisation. L'angle proposé ici est différent. Le présent article lève le voile sur les transformations menées afin d'améliorer la prise en compte de la sécurité au gré des différentes générations de réseaux mobiles, en répondant aux attentes des clients, en capitalisant sur les incidents de sécurité passés, en intégrant les évolutions technologiques et en s'adaptant aux évolutions du contexte (géopolitique, réglementaire). Ensuite, il explicite comment les opérateurs intègrent la sécurité dans le contexte de la 5G avec des exemples concrets. Enfin, il ouvre des perspectives sur la sécurité de la 6G.

1 Introduction

La plupart des articles relatifs à la sécurité des réseaux mobiles portent sur l'interface radio ou sur la signalisation. Il ne s'agit que d'un sous-ensemble des aspects gérés par les opérateurs. Tout d'abord, le présent article rappelle les principes de fonctionnement des réseaux mobiles (partie 2). Il présente ensuite les différentes générations des réseaux mobiles (partie 3) avant de se focaliser sur leur sécurité, les vulnérabilités associées et les incidents marquants (partie 4). A ce stade de l'article, il nous est possible de constater que chaque génération a permis une offre plus riche de services, a contribué à l'amélioration de la sécurité sur les différents segments, mais a aussi vu apparaître de nouvelles surfaces d'attaques. L'article montre alors comment cette évolution technique associée à l'évolution des services, du contexte géopolitique et réglementaire a donné un rôle majeur à l'opérateur dans la sécurité du réseau, et au delà, dans la société au point de devenir une activité vitale à la nation (partie 5). Il montre ensuite comment les opérateurs cherchent à répondre à ces nouveaux enjeux avec un premier retour opérationnel sur la 5G (partie 6). Il ouvre enfin des perspectives sur les premiers travaux réalisés sur la sécurité dans le contexte de la 6G (partie 7).

2 Principes généraux d'un réseau mobile

La principale caractéristique d'un réseau mobile est la capacité de fournir une connectivité réseau pour un terminal en mobilité, que ce soit sur le réseau de l'opérateur qui porte l'offre commerciale du client ou sur le réseau d'un opérateur tiers (roaming, par exemple à l'étranger). Le service offert peut être un service de téléphonie/voix, un service de messagerie de type SMS - Short Message Service - ou un service de transmission de données (DATA) au sens générique (accès Internet ouvert, isolation dans un VPN donnant accès à l'Intranet d'une entreprise, etc.). Le terminal mobile est usuellement appelé UE - User Equipement (le terme MS - Mobile Station était historiquement utilisé). Le réseau mobile est composé de deux parties, une partie qui gère la connectivité radio appelée RAN - Radio Access Network, et une partie cœur de réseau appelée CN - Core Network.

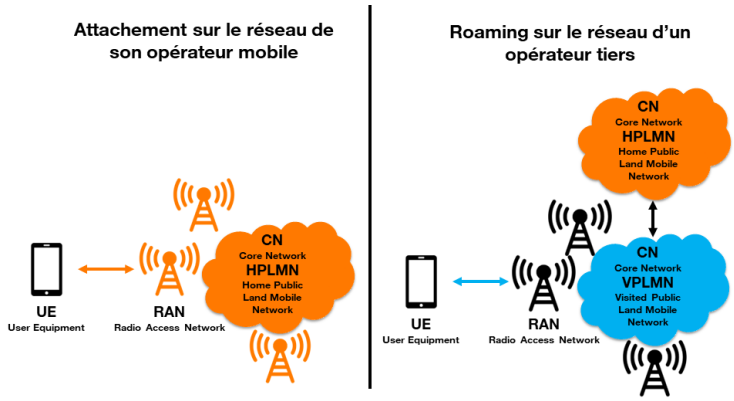

Fig. 1. Réseau mobile : Architecture générique d'un réseau mobile

L'UE est en continu à l'écoute des différents signaux radio afin de déterminer quel est le signal le plus pertinent parmi les signaux émis par les antennes voisines. Il peut ainsi à tout moment effectuer une mobilité vers une nouvelle antenne, en lien étroit avec le réseau mobile. Dans le contexte du roaming, il est courant de distinguer le réseau qui porte commercialement le client appelé HPLMN - Home Public Land Mobile Network, et le réseau visité appelé VPLMN - Visited Public Land Mobile Network. Il est enfin commun de distinguer 4 types de flux. Tout d'abord le plan usager (ou plan de données) correspond au trafic des clients (voix /

DATA) du réseau mobile. Ensuite, le plan de contrôle (appelé aussi plan de signalisation) englobe les flux qui permettent d'identifier / d'authentifier les UE, les flux nécessaires à la gestion de la mobilité, etc. Le troisième type de flux porte le provisionning des équipements depuis le système d'information commercial et technique des opérateurs. Le dernier type de flux concerne les accès en administration vers les équipements / les applications du réseau mobile ou encore les flux de supervision. Il s'agit du plan d'administration.

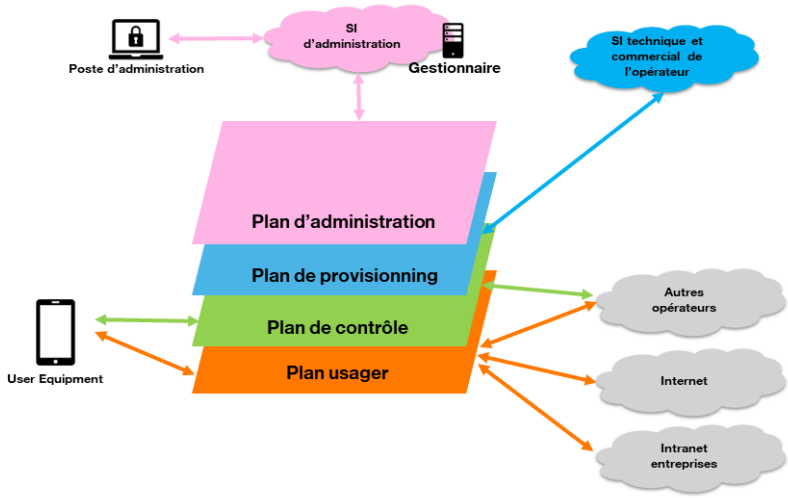

Fig. 2. Réseau mobile : Modélisation en plans d'un réseau mobile

3 Approche fonctionnelle des différentes générations de réseau mobile

3.1 1G : Les premiers réseaux mobiles

R150 et R450 : Le téléphone mobile de voiture Plusieurs réseaux téléphoniques mobiles ont été déployés dans le monde au cours du XX^{ème} siècle. Le premier réseau téléphonique mobile a ouvert commercialement en France en octobre 1955. Il s'agit du R150 qui permettra à quelques centaines de clients de téléphoner depuis une voiture, uniquement à Paris et dans la proche banlieue. Le service est à ses débuts entièrement manuel : tous les appels passent via l'unique Central Téléphonique Radio de Paris Ménilmontant et nécessite l'intervention des opératrices pour mettre en relation l'émetteur de l'appel et le récepteur.

Fig. 3. A gauche, un des premiers véhicules (Citroën DS19 - modèle 1956) équipés du Radiotéléphone Thomson-CSF R150 entièrement manuel, d'une puissance d'émission de 10 watts et d'un combiné d'appel du type PTT 1924 (source Orange/-DANP - Direction de l'Archivage Numérique et Patrimonial). A droite, téléphone de voiture de 1971 également de type R150 (source Orange/DANP)

Le R150 sera automatisé en 1973 et complété par le R450 avec une couverture géographique étendue aux principales villes régionales. Le réseau combiné R150+R450 comportera en 1984 jusqu'à 10 000 clients.

Radiocom 2000 : la 1G Radiocom 2000 sera lancée en 1986. Ce nouveau réseau téléphonique mobile est semi-analogique et semi-numérique à structure cellulaire. Il est considéré comme étant de la 1G - 1ère génération. Il reste en grande partie adossé au réseau téléphonique fixe "commuté" [26]. Il dépassera 200 000 clients et proposera une couverture

nationale. Néanmoins, il convient de garder en mémoire que, en communication, la mobilité entre cellules radio n'était pas assurée à ses débuts : le changement de cellule radio entraînait une coupure de la communication en cours et nécessitait de rappeler son correspondant pour poursuivre l'appel téléphonique. Il faudra attendre le début des années 1990 pour que soit ajoutée une nouvelle fonction permettant le transfert automatique intercellulaire des appels et donc une vraie continuité de service en mobilité sur le réseau de l'opérateur.

Fig. 4. A gauche, le terminal Radiocom 2000 (1989, source Orange/DANP) et à droite la carte de couverture Radiocom 2000 en 1990 (source Orange/DANP)

3.2 2G : GSM, GPRS et EDGE

La 2G en quelques mots Le GSM - Global System for Mobile communication, appelé par la suite 2G, a été spécifié à la fin des années 1980 - début des années 1990. Les principaux services rendus étaient un service téléphonique, la voix, basé sur un cœur mobile CS - Circuit-Switched - auquel a été ajouté un service d'envoi de message texte, le SMS, en détournant des fonctions de signalisation. Ensuite viendra l'ajout de service DATA au début des années 2000 avec la 2,5G appelée GPRS - General Packet Radio Service - puis la 2,75G appelée EDGE - Enhanced Data Rates for GSM Evolution. Le service DATA nécessite un cœur mobile PS - Packet Switched - et reste limité à quelques centaines de kb/s. La 2G amène cependant une restriction de l'usage car dès lors que le client passe ou reçoit un appel téléphonique, l'usage voix est prioritaire sur l'usage data sur les réseaux non DTM (Dual Transfer Mode). Il ne peut alors plus utiliser le service DATA durant sa conversation téléphonique. La mobilité évolue également par rapport à la 1G. La 2G rend possible la

mobilité, non seulement au sein du réseau de l'opérateur mais également en roaming, depuis un opérateur tiers.

Fonctionnement de la 2G Le document d'architecture [76] de 1992 décrit les principaux composants et les principales interfaces. L'UE se connecte sur le RAN composé des antennes radio, les BTS - Base Transceiver Station, contrôlées par les BSC - Base Station Controller. Pour le service voix, la signalisation est relayée par la BSC au commutateur MSC - Mobile-service Switching Center. Le MSC va gérer la mobilité et échanger avec le HLR - Home Location Register. Le HLR dispose de la base de données des clients. Il est provisionné par le SI technique et commercial de l'opérateur. La communication voix à proprement parler va passer par la MGW - Media GateWay.

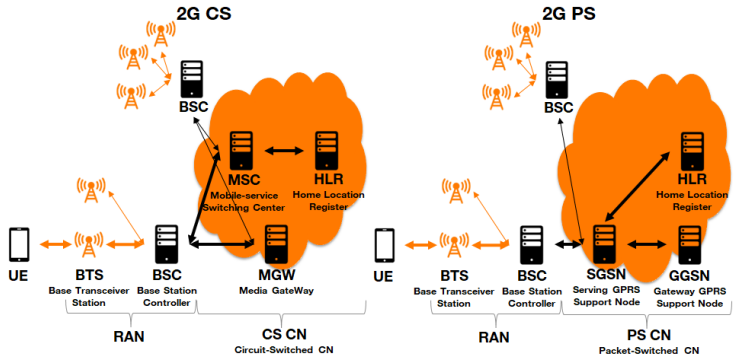

Fig. 5. Architecture 2G simplifiée en mode CS et en mode PS

Pour le service DATA, la signalisation et le trafic DATA de l'UE sont relayés par le BSC au SGSN - Serving GPRS Support Node. Par analogie au MSC, le SGSN va gérer la mobilité et échanger avec le HLR. Le trafic des clients va être encapsulé dans un protocole spécifique appelé GTP - GPRS Tunneling Protocol - entre le SGSN et le GGSN - Gateway GPRS Support Node. Le GGSN va porter l'interface externe au réseau mobile - typiquement Internet ou l'Intranet d'une entreprise.
La signalisation entre les différents composants du cœur de réseau 2G se base sur le protocole SS7 - Signalling System #7. En 1G, la mobilité se restreignait au réseau de l'opérateur. La 2G va permettre la mobilité entre réseaux mobiles, appelée itinérance ou roaming. En cas de roaming, le réseau VPLMN sur lequel est attaché l'UE au niveau RAN va échanger

avec le réseau HPLMN qui gère l'UE au niveau commercial via le protocole SS7. La relation entre VPLMN et HPLMN fait l'objet d'accords commerciaux entre opérateurs.

3.3 3G : UMTS

La 3G en quelques mots En Europe, la 3G se base sur l'UMTS - Universal Mobile Telecommunications System. La plupart des travaux de spécification a lieu à la fin des années 1990 - début des années 2000. L'accent est mis sur la montée en débit au niveau des interfaces radio. L'UMTS bénéficiera d'évolutions (HSPA - High Speed Packet Access) pour atteindre des débits "DATA" de plusieurs dizaines de Mb/s. Le service "DATA" offre alors des débits suffisants pour faire émerger de nouveaux usages, notamment la diffusion de vidéo.

Fonctionnement de la 3G D'un point de vue technique, la 3G reprend les briques du cœur de réseau 2G en maintenant une dualité entre cœur CS et cœur PS. Le RAN est appelé UTRAN - Universal Terrestrial Radio Access Network. Il est composé des antennes radio appelées NodeB ou NB et du contrôleur RNC - Radio Network Controller.

3.4 4G : LTE

La 4G en quelques mots Dans les années 2000, le 3GPP a défini la 4ème génération de réseau mobile, appelée LTE - Long Term Evolution. L'accent est tout d'abord mis sur la montée en débits de la "DATA" pour dépasser une centaine de Mb/s. Ensuite, la latence est également améliorée. Cette notion de latence englobe différents aspects comme le délai pour activer une connexion entre l'UE et le réseau ou le temps que met une donnée pour transiter via le réseau mobile. Enfin, une dernière évolution latente concerne la voix. En effet, la spécification de l'IMS - IP Multimedia Subsystem [7] et les implémentations sont alors suffisamment matures pour ouvrir la possibilité de faire de la VoIP - Voix sur IP - via le canal "DATA" de la 4G. Il s'agit de la VoLTE - Voice over LTE. La VoLTE a commencé à être commercialisée en France en 2016.

Fonctionnement de la 4G La 4G apporte plusieurs évolutions techniques importantes par rapport à la 3G, à commencer par le passage en tout IP des interfaces du réseau mobile et la création d'un nouveau cœur EPS - Evolved Packet System [4]. Côté RAN (appelé en 4G E-UTRAN -

Evolved Universal Terrestrial Radio Access Network), le composant actif des antennes est désormais appelé eNodeB. Les eNodeB sont raccordées en IP avec le cœur de réseau EPS. La MME - Mobile Management Entity - sert de point d'attachement à la signalisation. Elle dialogue directement avec l'UE via la signalisation NAS (Non-Access Stratum) qui traverse eNode B de manière transparente et elle échange avec le HSS - Home Subscriber Server (équivalent au HLR en 2G/3G) pour récupérer le profil de l'UE et les données d'authentification. Au niveau de la signalisation, le protocole SS7 utilisé en 2G ou en 3G, est remplacé par Diameter en 4G [62]. Le trafic utilisateur encapsulé dans le protcole GTP passe de son côté par la S-GW - Serving GateWay - du réseau visité (VPLMN) puis par le P-GW - Packet data network Gateway - avant de sortir vers la sortie IP prévue (Internet, Intranet d'une entreprise, IMS). La P-GW peut être côté HPLMN (cas "Home Routed") ou côté VPLMN (cas LBO - "Local BreakOut", le trafic ne remonte pas alors jusqu'au HPLMN, mais sort au niveau du réseau visité). Le PCRF - Policy and Charging Rules Function - est enfin chargé d'appliquer les modalités d'usage prévues par UE.

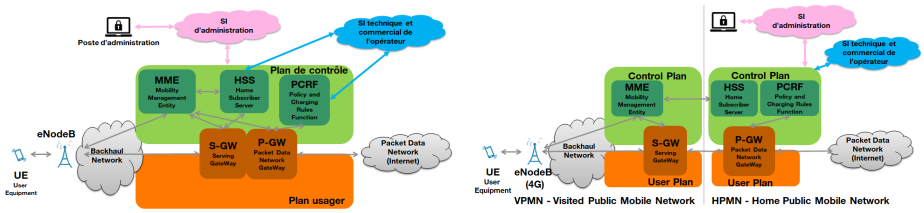

Fig. 6. Architecture 4G : connexion depuis le HPMN (à gauche) ou en roaming depuis un VPMN (à droite) en mode "Home routed"

3.5 5G

La 5G en quelques mots Le 3GPP a travaillé dans les années 2010 sur trois différentes promesses pour la 5G : augmenter les débits à l'accès, réduire les temps de latence et étendre les capacités de raccorder des objets connectés. Outre ces promesses services, la 5G représente une rupture majeure dans la conception de son cœur de réseau avec l'introduction d'une architecture basée "services" et un déploiement de ressources à la demande possible grâce à la virtualisation et l'automatisation des fonctions réseaux. Cette rupture a conduit le 3GPP à normaliser plusieurs options

de déploiement pour la 5G [5], permettant ainsi un déploiement progressif des nouveautés introduites en 5G.

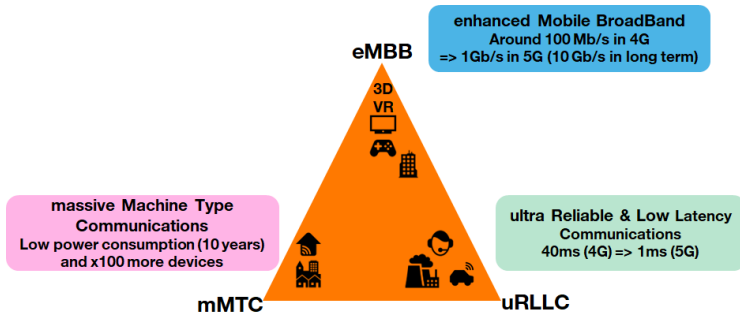

Fig. 7. Les promesses de la 5G

5G NSA Le mode 5G NSA - Non Stand-Alone - option 3X permet de déployer la "5G NR - Nouvelle Radio" sous la forme d'une gNodeB positionnée comme ressource secondaire d'une eNodeB. Le cœur reste un cœur 4G. L'intérêt de ce mode 5G NSA est d'offrir une montée en débit au niveau radio (lien UE-gNodeB) et d'avoir pu proposer aux clients, dès 2020 en France, des débits de l'ordre de 1 Gb/s.

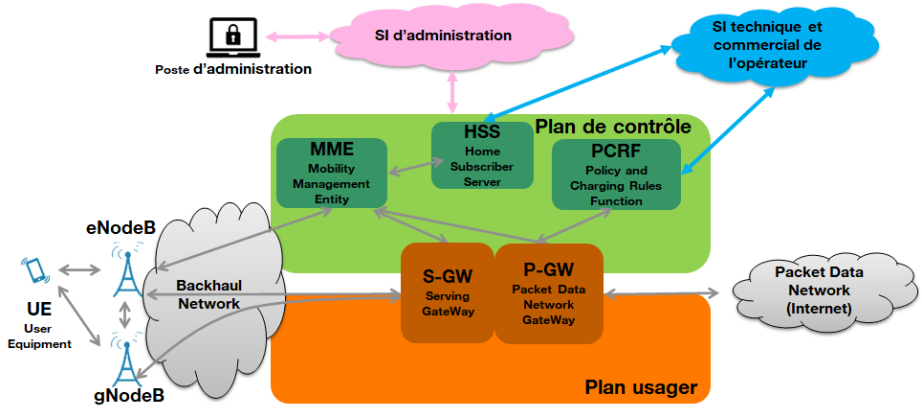

Fig. 8. Mode 5G NSA option 3X

5G SA

La "vraie" 5G Le mode 5G SA - Stand-Alone - options 2 est le seul mode qui permet de profiter pleinement des fonctionnalités de la 5G. Les opérateurs français devraient ouvrir des offres dans ce mode 5G SA d'ici la fin de l'année 2023. Il utilise la 5G NR (donc les gNodeB) sur un cœur 5G. Les documents pertinents sont ici l'architecture du système 5G [8], les procédures du système 5G [9] et le contrôle des usages et le mécanisme de facturation basé sur la consommation [10].

Un cœur 5G virtualisé Une première évolution structurelle concerne l'implémentation du cœur 5G. La plupart des fonctions sont virtualisées sous forme de machines virtuelles (VM) ou de conteneurs. Elles peuvent potentiellement être instanciées à la demande pour, par exemple, faire face à un besoin d'accroissement capacitaire ou pour permettre l'ouverture d'un nouveau service. La virtualisation des fonctions réseaux n'est que la partie visible de l'iceberg qui peut inclure aussi des fonctions de type SDN - Software Defined Networking -, la mise en oeuvre de l'automatisation ou encore de chaines CI/CD - Continuous Integration/Continuous Delivery or Deployment.

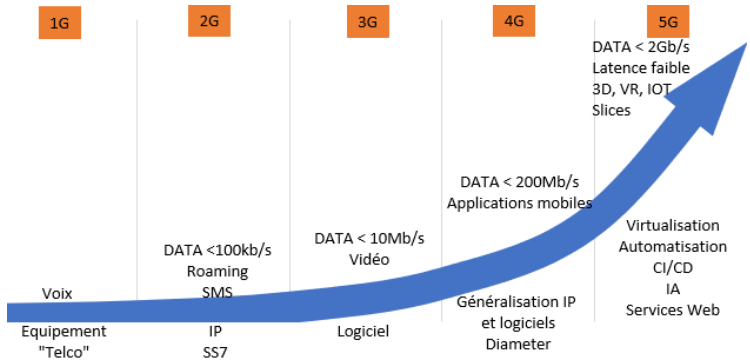

Fig. 9. Évolution de la complexité des services et des technologies mises en œuvre

Des fonctions à consommer La signalisation du cœur 5G est désormais basée sur des services web mis à disposition via des interfaces SBI - Service Based Interface - qui peuvent être consommés via un bus HTTP/2. L'architecture de ce bus est appelée SBA - Service Based Architecture. La liste des services exposés sur le bus de signalisation est tenue à jour et consultable au niveau de la NRF - Network Repository Function.

Des slices La spécification 5G SA prévoit la définition de slices c'est à dire des ressources logiques dédiées pour un service mobile. Il est possible de faire une analogie avec les routeurs virtuels et les réseaux privés virtuels de type L3VPN - Layer 3 Virtual Private Network sur les réseaux fixes. La sélection d'un slice passe par une nouvelle fonction, NSSF - Network Slice Selection Function.

Une séparation de la signalisation et du plan usager Lors de la connexion d'un UE à un réseau 5G, la première fonction cœur 5G que voit l'UE est la fonction AMF - Access and Mobility management Function - dont le rôle est assez proche de la MME en 4G. L'AMF gère l'attachement de l'UE au réseau du point de vue de la signalisation. L'AMF va d'abord solliciter une identification et une authentification de l'UE auprès de l'AUSF - AUthentication Server Function. Puis elle récupère le profil de l'UE auprès de la fonction UDM - Unified Data Management. Elle va ensuite piloter l'ouverture d'une session DATA en sollicitant la fonction SMF - Session Management Function. Le plan usager est géré par une fonction dédiée, l'UPF - User Plane Function - qui s'apparente à une partie des fonctions S-GW et P-GW en 4G. L'UPF est pilotée par une fonction du plan de contrôle (ou de signalisation) : la SMF.

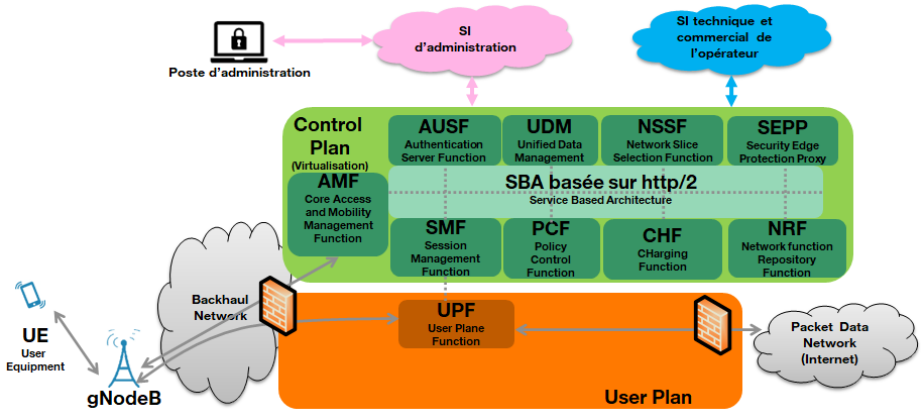

Fig. 10. Vue simplifiée du mode 5G SA option 2

Gestion des usages et facturation La gestion des usages associés à un UE donné est désormais assurée par une fonction PCF - Policy Control Function. Elle est distincte de la fonction CHF - CHarging Function - qui collecte les consommations dans l'optique d'alimenter la facturation.

4 Évolution de la sécurité dans les réseaux mobiles

Après la description fonctionnelle des différentes générations de réseau mobile, la présente section se focalise sur la sécurité. Elle explicite les principes de sécurité définis pour chaque génération et identifie les incidents (vulnérabilités ou attaques) connus. Elle montre ainsi comment chaque génération de réseau mobile a capitalisé sur la génération précédente.

4.1 1G, une première base

1G : sécurité La sécurité en 1G se limite à l'identification des clients. La surface d'attaque en 1G porte principalement sur l'interface radio. Or, dans le cas des clients Radiocom 2000, ils sont simplement identifiés et il n'y a pas de chiffrement des communications.

1G : vulnérabilités L'absence de chiffrement a été utilisée par des tiers, journalistes ou officines, pour écouter des communications téléphoniques entre clients en utilisant des scanners adaptés.

4.2 2G, capitalisation sur l'expérience de la 1G

2G : sécurité

Besoin en termes de sécurité L'expression du besoin en matière de sécurité [77] capitalise sur l'expérience de la 1G. Les besoins couverts par le réseau 2G restent élémentaires : protéger l'identité des UE en confidentialité, authentifier les UE, protéger en confidentialité la signalisation et les communications entre l'UE et le RAN.

Identification de l'UE L'UE présente au réseau son identifiant unique IMSI - International Mobile Subscriber Identity (le format est spécifié dans [78]) en clair. L'IMSI est utilisé au niveau de tous les noeuds du réseau pour identifier l'UE, en particulier au niveau du HLR, la base de données des UE. Lorsque l'UE se connecte, le HLR vérifie si l'IMSI de l'UE est connu ou non. Afin de limiter la transmission de l'IMSI au niveau de l'interface radio, une fois l'UE identifié, un identifiant local et temporaire est généré et utilisé dans la suite des échanges. Il est appelé TMSI - Temporary Mobile Subscription Identifier.

Authentification de l'UE et chiffrement Pour chaque UE, le HLR stocke le profil réseau associé, l'identité des MSC et SGSN traitant l'UE, la clé secrète K_i de l'UE et son MSISDN - Mobile Station International Subscriber Directory Number (= le numéro de téléphone en +33xxxxxxxxx). De plus, le HLR intègre usuellement les fonctions cryptographiques nécessaires AuC ou AC - Authentication Centre. Le HLR va calculer un nombre aléatoire RAND qui va servir de challenge. Puis le HLR calcule le résultat attendu du challenge SRES et la clé de chiffrement temporaire K_c en utilisant la clé secrète K_i de l'UE et RAND. Il transmet ensuite le triplet (RAND, SRES et K_c) au MSC. Le MSC relais uniquement le challenge RAND à l'UE et attend sa réponse. Cette méthode permet de préserver la confidentialité des clés K_i et de ne transmettre en interne du réseau de l'opérateur ou à un opérateur tiers (roaming) qu'une clé temporaire K_c valable jusqu'à la prochaine procédure d'authentification de l'UE (et donc la génération d'un nouveau challenge RAND).

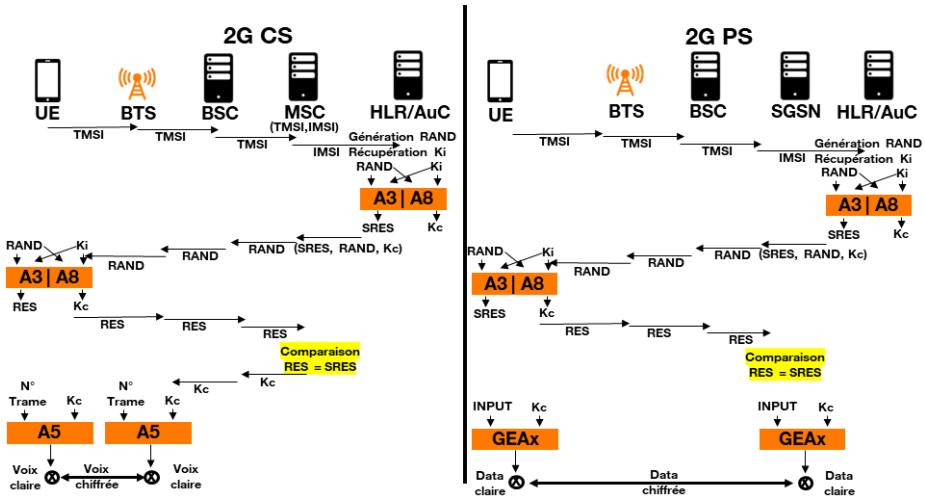

Fig. 11. Cryptographie en 2G

L'UE va utiliser sa clé secrète K_i et le challenge RAND pour calculer le résultat du SRES et remonter le résultat au MSC. Le MSC va comparer SRES et RES. Si les deux valeurs sont identiques, l'UE sera authentifié et le MSC pourra redescendre la clé K_c au BSC puis BTS afin de l'utiliser pour chiffrer les échanges avec l'UE sur l'interface radio. L'UE va calculer en parallèle cette même clé K_c et l'utiliser pour chiffrer les échanges avec

la BTS. Côté service DATA, le SGSN réalise les mêmes opérations que le MSC pour la partie authentification, mais la partie chiffrement est gérée directement entre le SGSN et le mobile contrairement au domaine CS. Le trafic entre l'UE et le SGSN est chiffré par des algorithmes similaires à ceux utilisés côté CS et appelés GEA - GPRS Encryption Algorithm. Différents choix sont possibles en termes de chiffrement de la voie radio :

- A5/0 côté CS, GEA0 côté PS : Absence de chiffrement
- A5/1 côté CS, GEA1 côté PS : Chiffrement faible (cassé)
- A5/2 côté CS, GEA2 côté PS : Chiffrement faible (cassé)
- A5/3 côté CS, GEA3 côté PS : Algorithme Kasumi [16] [17] [18]
- A5/4 côté CS, GEA4 côté PS : Algorithme Kasumi (variante) [19]

Identification des terminaux La 2G a introduit un mécanisme d'identification des terminaux basé sur IMEI - International Mobile Equipment Identity. Cette identité va remonter au niveau de la signalisation et elle fera l'objet d'une vérification au niveau de l'EIR - Equipment Identity Register - une base de données utilisé pour identifier les terminaux volés que l'opérateur doit bloquer.

2G : vulnérabilités

Les fausses stations de base dès 1993 Si l'UE est authentifié par le réseau lorsqu'il souhaite accéder au service, ce n'est pas réciproque : n'importe quelle BTS peut se faire passer pour une BTS légitime. Dès 1993 ([31], [36], [37]), sont apparus des équipements qui simulent une fausse BTS et permettent ainsi de récupérer l'ensemble des IMSI dans leur zone de couverture radio. Ces équipements appelés "IMSI Catcher" sont vendus par des fournisseurs comme Rhode & Schwarz (équipement appelé GA 090) ou Harris Corp (la gamme de produit qui prendra le nom de Stingray). Une fois l'IMSI récupérée, l'IMSI Catcher peut simuler côté réseau mobile, le fonctionnement de l'UE et côté UE le fonctionnement du réseau mobile en profitant de la transmission en clair du challenge aboutissant au calcul de la valeur RES et de la sélection du mode A5/0 (absence de chiffrement des communications) possible.
Rapidement, les IMSI Catcher ont ainsi intégré des fonctionnalités complémentaires comme l'interception des communications. De fait, ces équipements utilisés par les agences de renseignement [48] sont très réglementés en France. Ils sont concernés par les articles 226-3, 226-15, R.226-3 et R.226-7 du code pénal (voir la section 5.4 relative à l'évolution réglementaire).

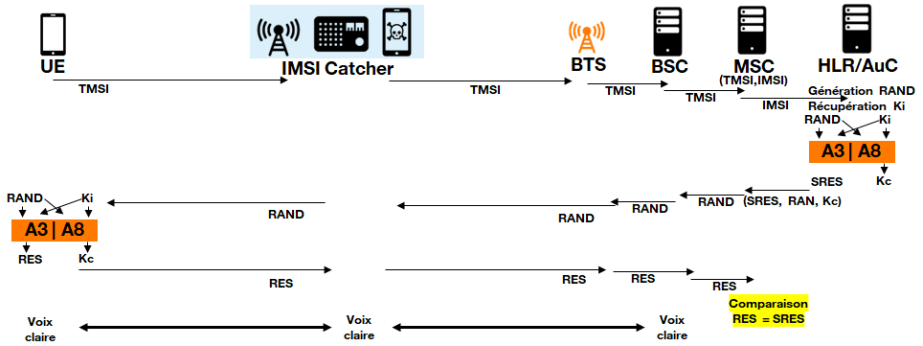

Fig. 12. Principes possibles de fonctionnement d'un IMSI Catcher

Transmission des clés de chiffrement K_c en clair entre le cœur et la BTS Une fragilité de la 2G est liée à la transmission de la clé de chiffrement K_c en clair entre le HLR et la BTS avec laquelle l'UE échange. Cette clé est facilement accessible, bas dans le réseau, jusqu'à la BTS.

2001 : compromission de la signalisation inter-opérateurs Les premiers signaux sur les vulnérabilités associées au protocole SS7 remontent au moins à 1993 [45]. Dès 2001, des vulnérabilités au niveau des réseaux 2G liées au manque de sécurité du protocole SS7 sont explicitées [38] : absence de sécurité dans les messages SS7 inter-opérateurs, équipements Telco trop permissifs dans leur capacité à répondre à des messages auxquels ils ne sont pas tenus de répondre, complexité de surveiller la signalisation SS7 au regard de la multiplication des interconnexions SS7 entre opérateurs, ouverture des interfaces SS7 à des nouveaux acteurs y compris des opérateurs "gris", etc. Un opérateur est considéré "gris" s'il profite d'une activité en grande partie légitime pour disposer d'interconnexion avec d'autres opérateurs, tout en offrant des services à des tiers potentiellement malveillants moyennant rémunération ou à des agences de renseignement étatiques. En 2008, le détournement des messages SS7 est exposé par Tobias Engel [32]. Il décrit comment, à partir du MSISDN, récupérer l'IMSI et la localisation de l'UE grâce au message MAP-SEND-ROUTING-INFO-FOR-SM [11]. Des attaques plus évoluées, intégrant notamment des scénarios de dénis de service, de détournement de communications et d'interception de communications seront décrites à partir 2014 par Tobias Engel [33], par Karsten Nohl [63] ou encore par Dmitry Kurbatov et Vladimir Kropotov [46].

4.3 3G, une sécurité renforcée au niveau de l'interface radio

3G : sécurité

Capitalisation sur l'expérience de la 2G De nouveaux objectifs de sécurité sont spécifiés pour la 3G [2]. Une analyse des risques a été réalisée en capitalisant sur l'expérience de la 2G pour déterminer les exigences sécurité de la 3G [1]. Un document est dédié à la description de l'architecture sous l'angle de la sécurité [6]. Les principales évolutions portent sur le renforcement de la sécurité au niveau de l'interface radio avec l'authentification du réseau et un contrôle de l'intégrité de la signalisation.

AKA - Authentication and Key Agreement La procédure AKA est décrite dans [6]. Le HLR/AuC calcule sur la base de l'IMSI de UE et de la clé K_i associée à cette IMSI

- Un challenge RAND.
- Le résultat du challenge $XRES = f2(RAND, K_i)$.
- Une clé $CK = f3(RAND, K_i)$ pour le chiffrement de la signalisation et de la DATA.
- Une clé $IK = f4(RAND, K_i)$ pour le contrôle d'intégrité de la signalisation.
- Une clé d'anonymisation $AK = f5(RAND, K_i)$.
- Un compteur anti-rejeu SQN_i - SeQuence Number - associé à cette IMSI et maintenu à jour côté HLR/AuC et côté UE.
- Une valeur $MAC = f1(SQN_i, RAND, AMF, K_i)$ où AMF - Authentication management field - est une valeur configurée dans le HLR/AuC assimilé à une version d'algorithme d'authentification.
- Le vecteur d'authentification $AUTN = SQNi \oplus AK||AMF||MAC$.

Le HLR/AuC transmet au MSC le vecteur d'authentification $AV = RAND||XRES||CK||IK||AUTN$. Le MSC relaie à l'UE les valeurs RAND et AUTN. Sur la base de sa clé K_i et des données fournies par le MSC, l'UE réalise les actions suivantes :

- Calcule de $AK = f5(RAND, K_i)$
- Extraction SQN_i à partir d'AUTN et de AK.
- Extraction de AMF et de MAC à partir d'AUTN.
- Calcule de $XMAC = f1(SQN_i, RAND, AMF, K_i)$: si $XMAC = MAC$ et si SQN_i est cohérent, alors le réseau est authentifié.
- Calcule des clés CK=f3(RAND,K_i) et IK=f4(RAND,K_i).
- Calcule du résultat du challenge $RES = f2(RAND, K_i)$ et transmission de RES au MSC.

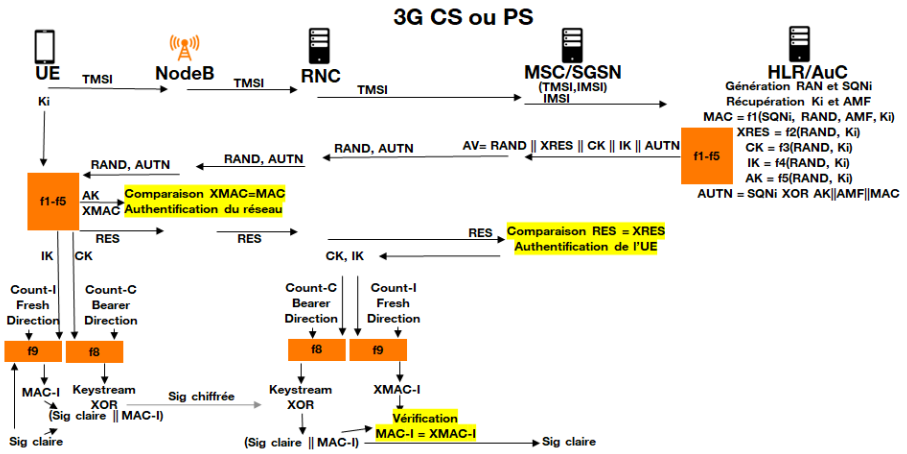

Fig. 13. AKA, chiffrement et contrôle d'intégrité de la signalisation en 3G

Le MSC peut alors vérifier si $RES = XRES$ et authentifier l'UE. Le MSC transmet alors les clés CK et IK au RNC. Contrairement à la 2G où le chiffrement était réalisé au niveau de la BTS, en 3G, le chiffrement et le contrôle d'intégrité sont réalisés plus haut dans le réseau, au niveau du RNC.

Intégrité de la signalisation En 3G, la signalisation bénéficie d'un mécanisme de contrôle d'intégrité obligatoire utilisant la clé IK obtenue avec la procédure AKA et un algorithme UIA - UMTS Integrity Algorithm. Il s'agit d'un progrès par rapport à la 2G. Le contrôle d'intégrité est réalisé au niveau du RNC côté réseau. Les algorithmes supportés sont UIA1 Kasumi [16] [17] et UIA2 Snow 3G [73] [72]. Il existe une exception où le contrôle d'intégrité peut ne pas être réalisé (section section 6.4.9 Emergency call handling de [6]). Dans ce cas particulier, il est question de l'algorithme UIA0 (absence de contrôle d'intégrité).

Absence d'intégrité du plan usager Aucun mécanisme de contrôle d'intégrité n'est prévu sur le plan usager en 3G.

Chiffrement de la signalisation et du plan usager Le plan usager et la signalisation bénéficient d'un mécanisme de chiffrement utilisant la clé CK obtenue avec la procédure AKA et un algortihme UEA - UMTS Encryption Algorithm. Le chiffrement/déchiffrement est réalisé au niveau du RNC côté réseau. Les algorithmes supportés sont UEA0 absence de chiffrement, UEA1 Kasumi [16] [17] et UEA2 Snow 3G [73] [72].

3G : vulnérabilités Malheureusement les mesures mises en place en 3G auront une efficacité très limitée.

Fausses stations de base (bis) Les fausses stations de base vont adapter leur stratégie afin de s'affranchir des mécanismes de protection introduits dans la 3G, notamment le mécanisme d'authentification mutuelle AKA et le contrôle d'intégrité de la signalisation. Une première option possible consiste à inciter l'UE à basculer en 2G. Une seconde option, plus compliquée, consiste à utiliser l'interconnexion inter-opérateurs SS7 pour faire passer la signalisation en clair et récupérer ainsi les vecteurs d'authentification (voir le paragraphe suivant).

Compromission de la signalisation inter-opérateurs (bis) Si les doutes sur la sécurité de la signalisation inter-opérateur SS7 apparaissent dès 1993 [45], il faudra attendre 2008 pour que des scénarios d'attaque soient exposés [32]. La spécification 3G au 3GPP est alors figée et la 3G déployée par les opérateurs. Les vulnérabilités décrites en 2G s'appliquent donc aussi en 3G.

4.4 4G, une refonte du modèle de sécurité

4G : sécurité La 4G fait évoluer le modèle de sécurité qui a prévalu en 2G/3G dans son document d'architecture de sécurité [15].

GUTI Le GUTI - Globally Unique Temporary UE Identity - est composé de deux parties. La première permet une identification globalement unique de la MME et la seconde permet une identification non ambiguë de l'UE (le TMSI) à l'instant t [20]. L'usage de l'identifiant temporaire GUTI permet de limiter la diffusion de l'identité permanente de l'UE, l'IMSI.

Cryptographie 4G Les principes sont décrits dans [15]. La 4G reprend le mécanisme AKA déjà utilisé en 3G. Le HSS calcule une clé K_{ASME} additionnelle à partir du triplet (CK, IK, $SQNi \oplus$ AK). Il transmet à la MME les valeurs RAND, XRES, AUTN et K_{ASME}. La MME est chargée de comparer le résultat du challenge RES calculer par l'UE avec la valeur XRES pour authentifier l'UE. La clé K_{ASME} est ensuite dérivée au niveau de la MME en une clé de chiffrement de la signalisation NAS K_{NASenc}, en une clé de contrôle d'intégrité de la signalisation NAS K_{NASint}, une clé eNodeB K_{eNB} qui doit être communiquée à l'eNodeB et un identifiant de la clé K_{eNB} NH - Next Hop parameter. La clé K_{eNB} est elle même dérivée au niveau de l'eNodeB pour obtenir la clé de chiffrement du plan usager

K_{UPenc}, la clé de chiffrement du plan de contrôle RRC K_{RRCenc} et la clé de contrôle d'intégrité du plan de contrôle RRC K_{RRCinc}. La protection du plan de contrôle (RRC et NAS) est assurée en confidentialité par l'EEA - EPS Encryption Algorithm - et en intégrité par l'EIA - EPS Integrity Algorithm :

— EEA0 et EIA0 correspond à l'absence de chiffrement et à l'absence de contrôle d'intégrité
— 128-EEA1 et 128-EIA1 pour l'algorithme SNOW 3G [73] [72]
— 128-EEA2 et 128-EIA2 pour l'algorithme AES (voir annexe B [15])
— 128-EEA3 et 128-EIA3 pour l'algorithme ZUC [75] [74]

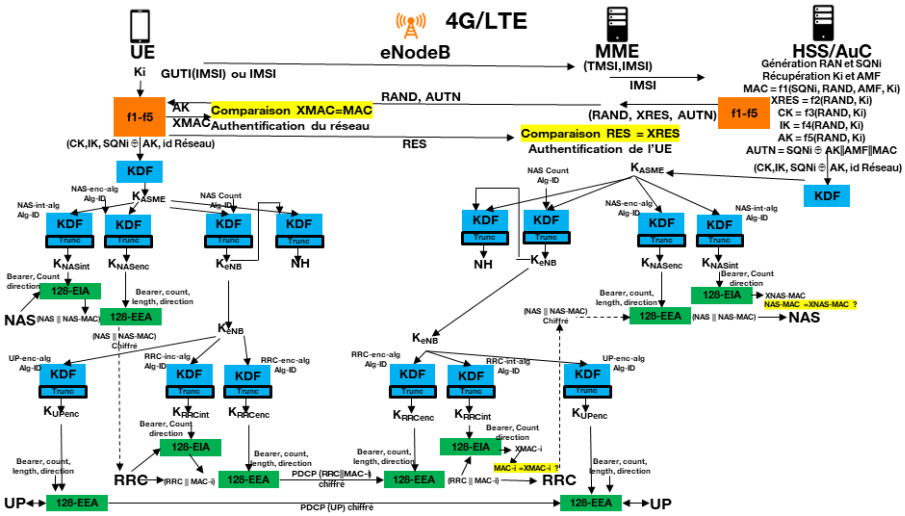

Fig. 14. Focus sur la cryptographie en 4G : cas d'une donnée envoyée par l'UE au réseau

Il convient ici de distinguer la signalisation NAS entre l'UE et la MME, de la signalisation RRC entre l'UE et l'eNodeB. La signalisation RRC peut être protégée en intégrité par EIA avec la clé K_{RRCinc} et chiffrée par EEA avec la clé K_{RRCenc}. La signalisation NAS peut être protégée en intégrité par EIA avec la clé K_{NASinc} et chiffrée par EEA avec la clé K_{NASenc}. Le message NAS authentifié et chiffré (NAS, NAS_MAC) est ensuite transmis à la couche RRC et donc potentiellement une nouvelle fois authentifié et chiffré au niveau RRC ((NAS,NAS_MAC),MAC_i). Concernant le plan usager UP, seul le chiffrement a été initialement proposé entre l'UE et l'eNodeB avec l'utilisation d'EEA et de la clé K_{UPenc}.

Pour les accès non-3GPP, une variante de l'algorithme AKA est définie. Il s'agit de l'EAP-AKA - Extensible Authentication Protocol method for 3rd Generation Authentication and Key Agreement [21].

Domaines de confiance et Security Gateway La 4G ouvre la possibilité de séparer la partie RAN (domaine qui n'est pas de confiance) de la partie cœur (domaine de confiance) avec une SEG - SEcurity Gateway (aussi noté SecGW) chargée de filtrer les flux, sur le plan d'administration, sur le plan de contrôle et sur le plan usager. La SEG authentifie les eNodeB avec IKEv2 et permet de monter des tunnels IPsec entre les eNodeB et les SEG afin protéger le trafic du plan de contrôle et du plan usager en confidentialité et en intégrité. Des mécanismes anti-rejeux sont enfin possibles [15] [13]. Pour cela, il est proposé aux opérateurs de mettre en place une infrastructure de gestion de clés publiques (PKI) et un mécanisme d'enrôlement automatique basé sur CMPv2 [14].

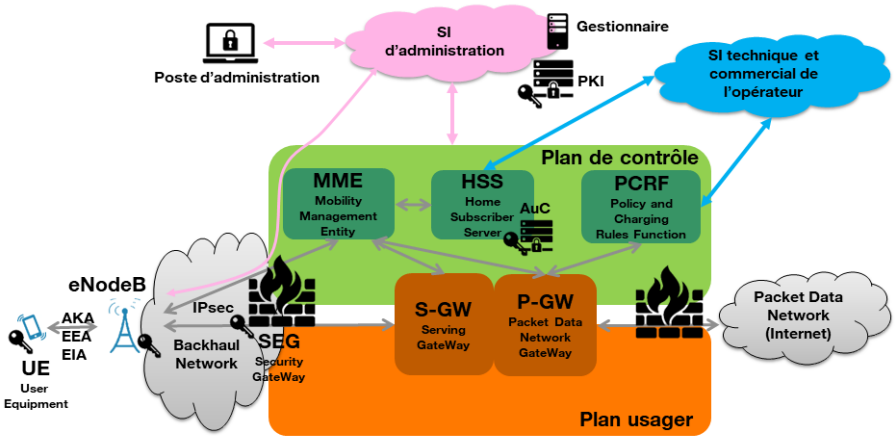

Fig. 15. Architecture sécurisée en 4G

Protection de la sortie WAN pour le trafic DATA La sortie WAN est habituellement protégée par un pare-feu. Outre le filtrage des flux (usuellement, seul le trafic à l'initiative de l'UE est autorisé), le pare-feu effectue aussi la translation d'adresse et de port afin de permettre le partage d'une adresse IPv4 publique entre plusieurs UE.

Signalisation inter-opérateur (non normatif) Dans les années 2010, les scénarios d'attaque vont se concrétiser. Si 3GPP n'a pas fait évoluer la normalisation pour traiter les problèmes, des contre-mesures sur l'interface de signalisation inter-opérateur vont s'affiner au niveau des implémentations. Tout d'abord, des contrôles élémentaires sur la signalisation SS7/Diameter ont été développés et configurés sur les équipements exposés pour interdire les messages SS7/Diameter qui n'ont pas lieu d'être sur une interco inter-opérateur. Ensuite des sondes de détection puis des pare-feu de signalisation ont été déployés au niveau des points d'interconnexion pour détecter et filtrer les messages SS7/Diameter manifestement non légitimes. Dans les deux cas, les paramétrages nécessitent un travail de fond non trivial afin de trouver les bons compromis entre la protection du réseau et éviter de filtrer des messages légitimes, l'Enfer étant dans les détails. Concernant spécifiquement les SMS, les opérateurs ont déployés des composants dédiés "SMS Home-Router" pour limiter la diffusion des IMSI réels. Une très bonne source sur la signalisation figure dans [62].

Durcissement (non normatif) Les fournisseurs ont progressivement durci les implémentations des fonctions 4G. Ils vont pour cela bénéficier des retours d'expérience des opérateurs et des contrôles/audits réalisés par les agences nationales de sécurité (en premier lieu l'ANSSI en France). Ce durcissement porte sur un renforcement de la sécurité du plan de management (entre le SI d'administration et les fonctions 4G) et sur le durcissement des OS/applications.

4G : vulnérabilités

Fausses stations de base (ter) Malheureusement les mesures mises en place en 4G auront une efficacité très limitée tant que le fall back en 2G est possible sur l'interface radio.

2016 : Compromission de la signalisation inter-opérateurs (ter) La possibilité de requêter en Diameter le HPLMN reste problématique. Plusieurs articles référencent en effet des attaques similaires à SS7 sur Diameter à l'image de l'usage de la procédure Diameter "Send Routing Info for SM" [12] pour récupérer une IMSI et la localisation d'un client à partir de son MSISDN [43].

2019 : Attaque sur la couche 2 du RAN Alors que les travaux de recherche sur la sécurité du RAN se focalisent habituellement sur la couche physique ou la couche 3, des chercheurs se sont intéressés à la couche 2 [71]. Dans

un premier temps, les chercheurs ont établi comment faire le lien entre l'identité de l'UE au niveau de la couche 2 (RNTI - Radio Network Temporary Identity) et l'identité du niveau 3 (TMSI voir IMSI) en écoutant les échanges entre l'UE et l'eNodeB. Dans un second temps, les chercheurs montrent comment en étudiant le trafic chiffré au niveau radio vers les principaux sites web (temps de réponse, taille des paquets, fréquence des paquets, etc.), il est possible de déterminer des signatures type par site. En observant le trafic chiffré d'un UE, il est alors possible de deviner par une approche statistique le site "consommé" au regard des précédentes signatures. Intervient alors l'attaque ${}_{A}LTE_{R}$. Une fois le trafic de l'UE identifié, il est possible de cibler le trafic DNS. L'attaque utilise ici la faiblesse de l'algorithme de chiffrement AES-CTR utilisé pour chiffrer le trafic UP et la connaissance d'une partie du texte clair d'une requête DNS à savoir l'adresse destination du serveur DNS proposé par défaut par l'opérateur. Il est alors possible de prévoir un masque qui vient transformer cette adresse IP destination "chiffrée" du serveur DNS en l'adresse IP du serveur pirate. Le serveur DNS pirate va alors répondre à la demande de résolution d'un nom de domaine par une adresse IP d'un serveur web compromis qui simulera le site web légitime.

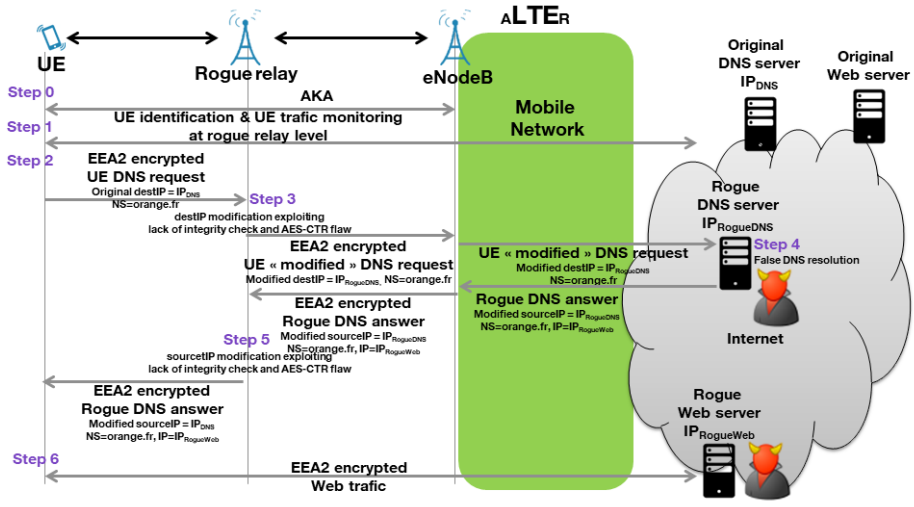

Fig. 16. ${}_{A}LTE_{R}$

4.5 5G NSA

La sécurité du mode 5G NSA option 3X est identique à la 4G. Il en va de même pour les vulnérabilités associées.

4.6 5G SA

5G SA : sécurité Le document fédérateur est le document de sécurité décrivant l'architecture et les procédures des systèmes 5G [22].

Confidentialité de l'identité des UE Le premier élément marquant concerne le traitement de l'identité du client, appelée SUPI - Subscription Permanent Identifier (= IMSI ou un autre identifiant) en 5G [8] [20]. Il est désormais possible de ne plus transmettre l'identité de l'UE en clair sur le réseau grâce à un mécanisme de chiffrement asymétrique basé sur les courbes elliptiques (annexe C.3 de [22]). L'UE connaît la clé publique de son HPLMN $K_{pubHPLMN}$ et génère un couple (clé privée K_{priv_e},clé publique K_{pub_e}) éphémère. Il va alors pouvoir calculer un secret éphémère partagé uniquement avec le HPLMN. Ce secret éphémère est utilisé pour dériver une clé de chiffrement éphémère EK - Encryption Key -, un compteur ICB - Initial Counter Block - et une clé de calcul d'intégrité éphémère MK - MAC Key. La clé EK permet de chiffrer le SUPI avec le compteur ICB et d'obtenir côté UE le SUCI - Subscription Concealed Identifier. La clé MK permet de calculer un motif d'intégrité MAC-tag du SUCI. L'UE envoie alors sa clé publique éphémère K_{pub_e}, le SUCI et MAC-tag à l'AMF via la signalisation NAS.
L'AMF va relayer le triplet à l'UDM/SIDF - Subscription Identifier Deconcealing Function. Une fois le motif d'intégrité vérifié et le SUPI déchiffré à partir du SUCI, l'UDM/SIDF va retourner le SUPI à l'AMF. L'AMF va générer une identité temporaire 5G-GUTI, l'associer au SUPI et la transmettre à l'UE après authentification de l'UE (voir paragraphe ci-dessous).
Ce nouveau mécanisme permet, tant que l'UE est en 5G, de protéger efficacement la confidentialité de l'identité des UE au niveau de l'interface RAN face à des IMSI Catcher. Il permet également au HPLMN de ne transmettre l'identité réelle de l'UE au VPLMN qu'après la procédure d'authentification AKA.

Authentification de l'UE et du réseau Les principes sont décrits dans [22]. La 5G reprend le mécanisme AKA déjà utilisé en 3G et en 4G. La fonction SEAF - SEcurity Anchor Function - de l'AMF du VPLMN fait une

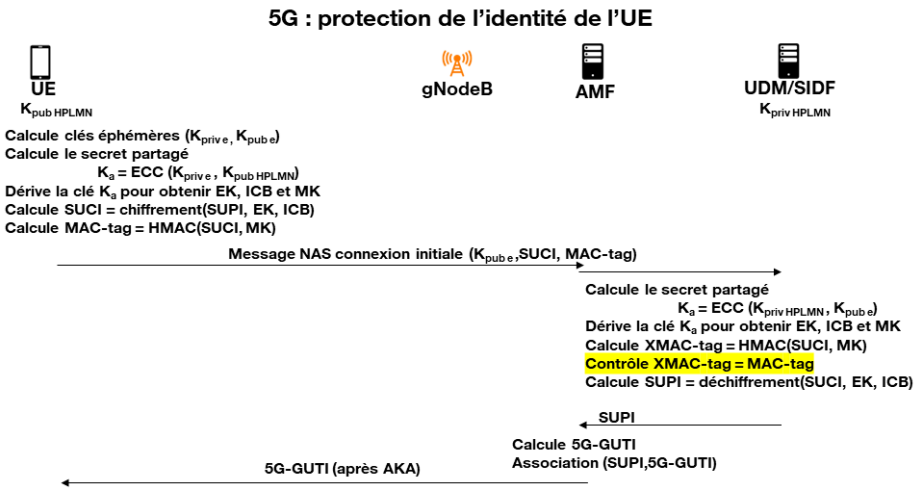

Fig. 17. Protection de l'identité des UE en 5G SA

demande de vecteur d'authentification auprès de l'AUSF du HPLMN. Pour cela, elle fournit l'identité du client (SUPI) et l'identifiant du réseau SN-name. L'AUSF relaie la demande à la fonction ARPF - Authentication credential Repository and Processing Function - de l'UDM. C'est l'ARPF qui calcule le vecteur d'authentification (RAND , XRES , CK , IK , AUTN) comme en 3G. Il existe ensuite deux variantes décrites dans la spécification 3GPP, EAP-AKA' (EAP - Extensible Authentication Protocol, méthode déjà présente en 4G pour les accès non 3GPP) et 5G-AKA. Cet article ne se focalisera que sur le 5G-AKA.

- L'ARPF dérive $XRES* = KDF(CK||IK, 0x6B, RAND, XRES)$.
- L'ARPF dérive $K_{AUSF} = (CK||IK, 0x6A, SNName, SQNi \oplus AK)$ où SN name est l'identifiant du réseau VPLMN.
- L'ARPF envoye ensuite à l'AUSF le quadruplet (RAND,XRES*,AUTN,K_{AUSF}).
- L'AUSF calcule $HXRES* = SHA256(RAND||XRES*)$.
- L'AUSF stocke le couple (SUPI, XRES) et envoie à la fonction AMF/SEAF du VPLMN le triplet (RAND,HXRES*,AUTN).
- La fonction AMF/SEAF du VPLMN va stocker le couple (SUPI,HXRES*) et envoyer (RAND,AUTN) dans la signalisation NAS au gNodeB qui fait suivre le message à l'UE en l'encapsulant dans la signalisation RRC .

— A la réception du message, l'UE calcule AK puis interprète la valeur AUTN et en déduit les valeurs SQNi, AMF et MAC. L'UE calcule ensuite la valeur $XMAC == f1(SQNi, RAND, AMF, K_i)$ et compare la valeur XMAC avec MAC. Si les deux valeurs sont identiques et si le compteur SQNi est cohérent, le réseau est authentifié par l'UE.
— Une fois le réseau authentifié, l'UE calcule la réponse RES = f2(RAND, K_i) puis la dérive en $RES* = KDF(CK||IK, 0x6B, RAND, RES)$. Cette valeur est remontée au réseau vers l'AMF/SEAF du réseau VPLMN.
— L'AMF/SEAF va calculer $HRES* = SHA256(RAND||RES*)$ et comparer le résultat avec la valeur HXRES* que lui avait communiqué l'AUSF du HPLMN. Si les deux valeurs sont identiques, alors l'AMF/SEAF du VPLMN a pu authentifier l'UE. Il va alors transmettre à l'AUSF la valeur RES*.
— L'AUSF va alors comparer RES* avec la valeur XRES* et si les deux valeurs sont identiques, alors l'AUSF a pu authentifier l'UE. Il signale à l'UDM le succès de l'authentification.

A ce stade, l'UE a authentifié le réseau HPLMN. Le VPLMN et le HPLMN, ont authentifié l'UE. Ce double niveau d'authentification côté réseau est une nouveauté apportée par la 5G.

Hiérarchie des clés 3GPP a défini une hiérarchie des clés, en partant du principe que le composant le plus sensible/protégé est l'UDM du HPLMN, puis dans l'ordre, l'AUSF du VPLMN, l'AMF/SEAF du VPLMN et enfin la gNodeB, le composant le moins sécurisé. Dès lors, 3GPP utilise un mécanisme de dérivation des clés pour que la compromission d'une clé au niveau d'une fonction 5G ne remette pas en question la sécurité des clés situées au dessus - au plus près de l'UDM. Une fois l'authentification réalisée, l'ARPF va fournir à l'AUSF la clé K_{AUSF}. La clé K_{AUSF} est stockée au niveau de l'AUSF et dérivée en K_{SEAF} = KDF (K_{AUSF},0x6C, SN name). La clé K_{SEAF} est transmise à l'AMF/SEAF du VPLMN qui va la stocker et l'utiliser pour calculer la clé K_{AMF} = KDF (K_{SEAF},0x6C,IMSI,ABBA=0x0000). La clé K_{AMF} va également être stockée au niveau de l'AMF/SEAF. Cette clé va servir à dériver :

— La clé K_{NASenc} utilisée pour le chiffrement de la signalisation NAS entre l'UE et l'AMF.
— La clé K_{NASint} utilisée pour garantir l'intégrité de la signalisation NAS entre l'UE et l'AMF.
— La clé K_{gNB} pour un gNodeB.

— La clé "Next Hop" K_{NH} à la première itération.

La clé K_{gNB} et la clé K_{NH} sont transmises au gNodeB sur lequel l'UE se trouve. La clé K_{gNB} est elle même dérivée au niveau de la gNodeB pour obtenir

— La clé K_{RRCenc} utilisée pour le chiffrement de la signalisation RRC entre l'UE et le gNodeB.

— La clé K_{RRCint} utilisée pour garantir l'intégrité de la signalisation NAS entre l'UE et le gNodeB.

— La clé K_{UPenc} utilisée pour le chiffrement de l'UP entre l'UE et le gNodeB.

— La clé K_{UPint} utilisée pour garantir l'intégrité de l'UP entre l'UE et le gNodeB.

Il est important de noter un progrès par rapport à la 4G : il est désormais possible de protéger le plan usager en intégrité.

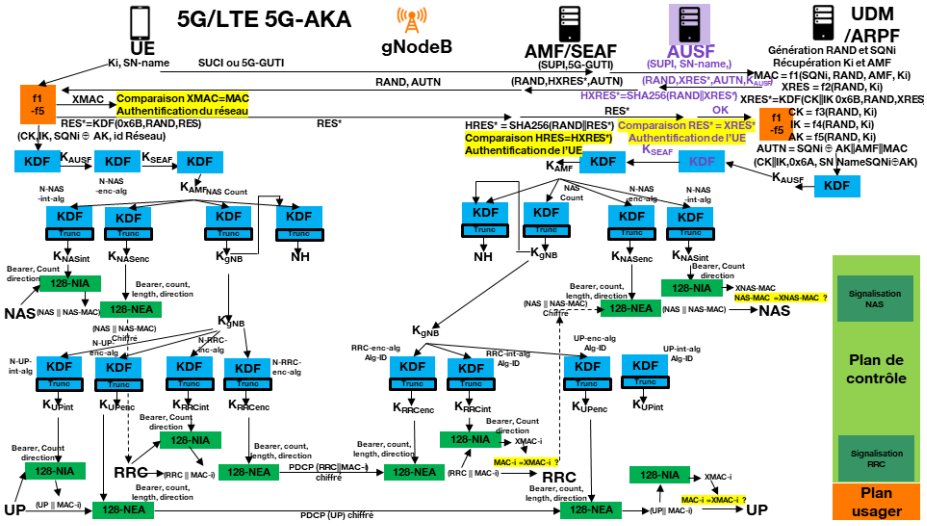

Fig. 18. 5G-AKA, hiérarchie des clés et chiffrement/contrôle d'intégrité

Chiffrement et authentification des échanges La protection du plan de contrôle (RRC et NAS) et la protection du plan usager (UP) sont assurées en confidentialité par le NEA - New-radio Encryption Algorithm for 5G - et en intégrité par le NIA - New-radio Integrity Algorithm for 5G. Ces algorithmes sont définits dans l'annexe D de [22] :

— NEA0 (identique à EEA0) et NIEA0 (identique à EIA0) correspond à l'absence de chiffrement et à l'absence de contrôle d'intégrité

— 128-NEA1 (128-EEA1) et 128-NIA1 (128-EIA1) pour l'algorithme SNOW 3G [73] [72]
— 128-NEA2 (128-EEA2) et 128-NIA2 (128-EIA2) pour l'algorithme AES (voir annexe B [15])
— 128-NEA3 (128-EEA3) et 128-NIA2 (128-EIA3) pour l'algorithme ZUC [75] [74]

Domaines de confiance et Security Gateway La 5G reprend le composant SEG et les fonctionnalités associées comme en 4G voir la section 4.4.

Sécurité du cœur de réseau L'architecture SBA - Service Based Architecture - du cœur de réseau repose sur des interfaces proposant des services web SBI - Service Based Interfaces. La fonction NRF - Network Repository Function - tient à jour la liste des fonctions disponibles, leur statut et leur profile. Toutes les fonctions 5G doivent supporter TLS avec une authentification mutuelle en se basant sur des certificats conformément à [14]. Les échanges sont ainsi protégés en confidentialité et en intégrité. Un mécanisme anti-rejeu doit également être implémenté au niveau SBI. Un composant optionel, SCP - Service Communication Proxy - permet de masquer la complexité du réseau et de router les messages de signalisation entre les fonctions du cœur 5G. Le SCP peut également jouer un rôle de proxy filtrant des messages de signalisation.

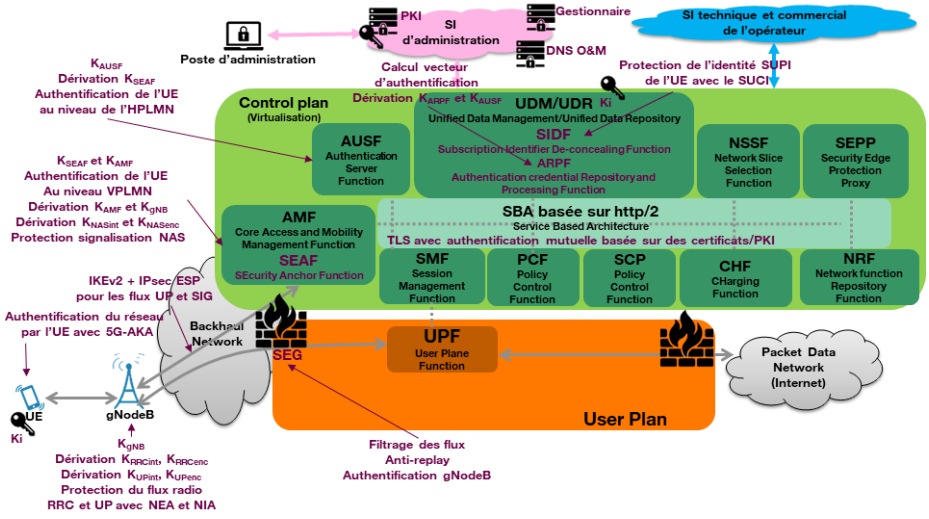

Fig. 19. Principaux points de sécurité dans la 5G SA

Sécurité au niveau de l'interconnexion inter-opérateur 3GPP a défini une nouvelle fonctionnalité pour protéger nativement la signalisation au niveau des interconnexions entre opérateurs. Il s'agit de la fonction SEPP - Security Edge Protection Proxy. La fonction SEPP permet de masquer la topologie du HPLMN, de filtrer les messages de signalisation et de protéger les échanges. SEPP peut ainsi réaliser une authentification mutuelle entre le SEPP VPLMN et le SEPP HPLMN, gérer les clés nécessaires pour ensuite chiffrer et garantir l'intégrité des échanges.

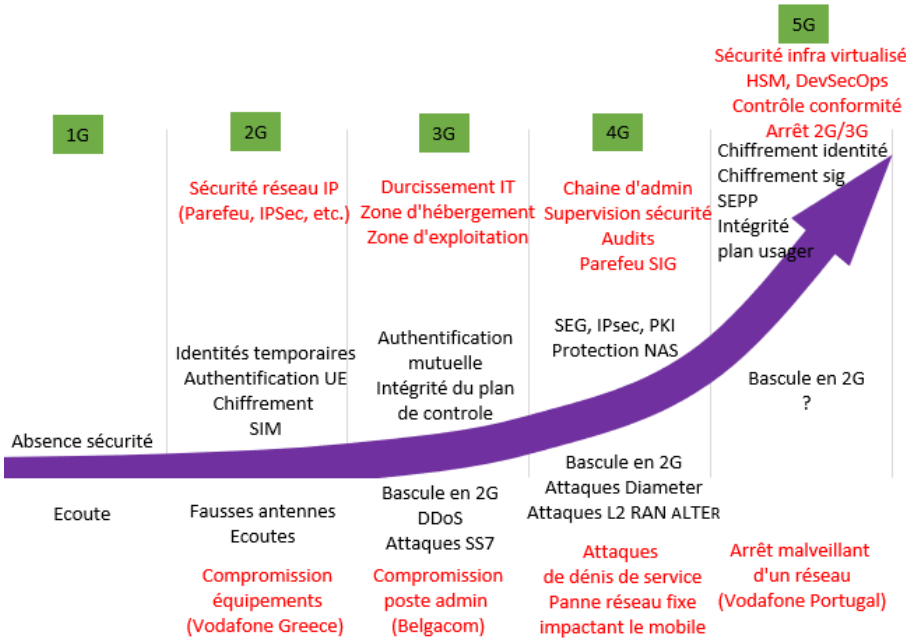

Fig. 20. Évolution des vulnérabilités et des contre-mesures mises en oeuvre

5G SA : vulnérabilités

2021 : Usage légal de fausses stations de base Le rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement publié en 2020 [48] et le rapport annuel de la Commission nationale de contrôle des techniques de renseignement publié en 2022 apportent quelques précisions sur l'usage des IMSI Catcher par les services compétents français. Ces dispositifs, dans le contexte prévu par le loi française, permettent notamment

de recueillir l'IMSI et l'IMEI des UE situés dans la zone de couverture (583 occurrences en 2021) et d'intercepter les correspondances (aucune occurrence en 2021). Le rapport [48] relate par ailleurs l'inquiétude des services compétents face au mécanisme de protection de l'identité des UE (SUCI) qui empêche les IMSI catcher de récupérer l'IMSI en 5G SA.

2022-2023 : Usage illégal de fausses stations de base Depuis quelques mois, des dispositifs similaires à des fausses stations de base ont été identifiés en France pour émettre des SMS frauduleux appelé aussi Smishing. Par hasard, les autorités françaises ont intercepté un premier véhicule contenant un équipement suspect le 30 décembre 2022 à Paris.[1] Il s'agissait en fait d'une fausse station de base. Les autorités françaises sont intervenus le 14 février 2023 pour interpeller les principaux protagonistes et saisir le matériel illégalement détenu et utilisé en France, notamment une seconde fausse station de base [65]. Une enquête judiciaire est en cours.

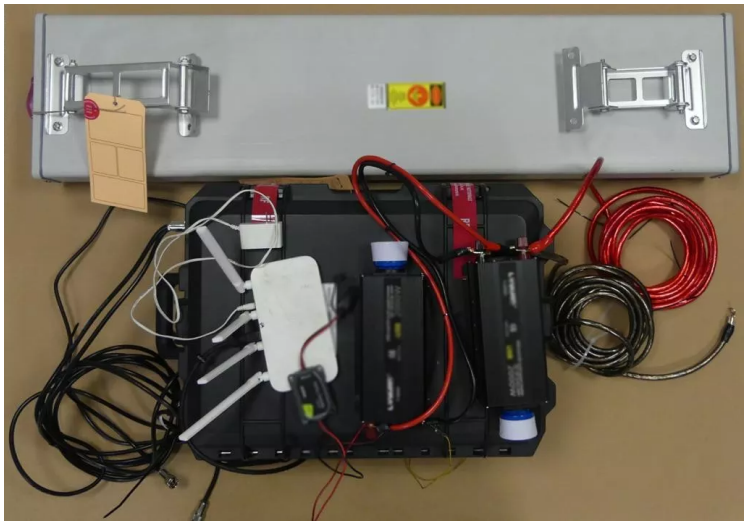

Fig. 21. IMSI Catcher (SIRPA gendarmerie, 2023)

[1] https ://twitter.com/AmauryBucco/status/1608931645587087360

5 Un rôle désormais majeur des opérateurs de réseau mobile dans la société

Les sections précédentes ont mis en exergue l'élargissement des services offerts par les opérateurs, une transformation des réseaux avec une frontière Telco/IT qui tend à disparaître mais aussi une évolution des problématiques sécurité qui couvrent désormais un domaine très large allant du secret des correspondances des clients jusqu'à l'intégrité et la disponibilité même du réseau global. Cette section complète cet état des lieux et montre comment l'évolution des attendus des clients et les changements des contextes géopolitiques, concurrentiels et réglementaires ont modifié les attentes autour de la sécurité des réseaux mobiles au point d'en faire des actifs "vitaux".

5.1 Les multiples attendus des multiples clients

Un besoin croissant en disponibilité Avec le développement des services proposés au cours des dernières décennies, le réseau mobile a pris une place prépondérante dans la société et dans l'économie. Les usages vont aujourd'hui bien au-delà de l'usage "loisir" du mobile perçu par le grand public. Les exemples ci-dessous illustrent le besoin croissant de disponibilité des réseaux pour les appels d'urgence ou pour le fonctionnement des entreprises, et la prise de conscience des politiques.

2012 : Impact d'un bug logiciel sur la disponibilité Le 6 juillet 2012, Orange France a du faire face à un dysfonctionnement de ses HLR impactant ses clients.[2] Il ne s'agit pas d'un acte malveillant mais bien d'un bug logiciel qui a impacté l'ensemble des instances de HLR pendant une dizaine d'heures. Le même stimuli a provoqué le même dysfonctionnement sur toutes les instances de HLR. Au-delà de l'incident technique et de l'impact pour les clients, un autre fait marquant n'est pas passé inaperçu. Pas moins de 3 ministres, Arnaud Montebourg (ministre du Redressement productif), Fleur Pellerin (ministre des PME et du Numérique) et Benoît Hamon (ministre de l'Économie sociale et de la Consommation), se sont relayés dans la salle de crise d'Orange. Ils ont rappelé le caractère crucial des communications électroniques dans la vie courante des Français et dans l'économie du pays [27].

[2] `https://www.dailymotion.com/video/xs4bs8`

2015 : indisponibilité du réseau mobile Orange Polska en raison d'une panne sur son réseau fixe Suite à un bug logiciel sur un équipement de collecte fixe, l'envoie d'une donnée de routage erronée au coeur de réseau fixe d'Orange Polska a créé un dysfonctionnement de son plan de contrôle le dimanche 23 mars 2015, vers 22h. Le réseau mobile d'Orange Polska étant adossé sur le réseau fixe, le réseau mobile n'était plus accessible. Pour des raisons similaires, la VoIP a également été impactée. L'indisponibilité de la VoIP et l'indisponibilité du réseau mobile ont compliqué la tâche de la supervision pour contacter les experts à même d'investiguer sur l'incident. Il aura fallu une dizaine d'heures pour localiser l'origine de l'incident et rétablir le réseau fixe, le réseau mobile et la VoIP. Les clients avaient de nouveau accès au réseau mobile le lundi 24 mars 2015 vers 8h.

2022 : Acte malveillant chez Vodafone Portugal Le 7 février 2022 à 21h, les services mobiles et la VoIP fixe de Vodafone Portugal se sont arrêtés brutalement [67]. La voix en 2G est remontée très rapidement, en 1h. La DATA 2G/3G est remontée à 8h le 8 février et la 4G est remontée à 20h mais avec des débits limités à 10 Mb/s et des instabilités. Il faudra attendre le 16 février 2022 pour un retour à la normal de la DATA 4G/5G et le 23 février 2022 pour le retour de la VoLTE. Que s'est-il passé ? Factuellement, aucun groupe de pirates n'a publiquement revendiqué une attaque sur Vodafone Portugal de cette nature et de toute façon, aucune attaque documentée jusque là ne portait atteinte à ce point à la disponibilité d'un réseau mobile. Par ailleurs, une communication interne de Vodafone Portugal expliquait le 18 février 2022, que nous ne saurons probablement jamais les motivations derrière cette attaque laissant planer le doute sur le fait que l'attaque aurait pour origine un individu et serait potentiellement interne à Vodafone Portugal ou à un sous-traitant de Vodafone Portugal. Aucune communication officielle de Vodafone Portugal ou des autorités portugaises n'a précisé la nature de l'attaque. Plusieurs interventions sur des forums officieux de discussion convergent sur une attaque ciblant les composants virtualisés : l'attaquant aurait arrêté méthodiquement toutes les fonctions réseau virtualisées puis les infrastructures support et aurait commencé à effacer les sauvegardes pour ralentir la restauration des VM lorsqu'il a été bloqué. Cet incident a été suivi de près par le gouvernement portugais à commencer par le premier ministre, António Costa [70].

2022 : indisponibilité du réseau mobile de Rogers Communication en raison d'une panne sur son réseau fixe Même si l'origine technique du bug est différente du cas Orange Polska en 2015, l'opérateur canadien Rogers Communication a rencontré une difficulté similaire le vendredi 8 juillet

2022 à savoir un dysfonctionnement du plan de contrôle du réseau fixe qui a entraîné un arrêt du réseau mobile [44]. Alors que l'incident a débuté vers 4h du matin, il aura fallu toute la journée aux équipes techniques de Rogers pour identifier l'origine de l'incident, reprendre la main sur les équipements concernés et corriger les configurations. Les services ont commencé à reprendre vers 20h et il faudra attendre le samedi 9 juillet pour une situation quasi-normale. François-Philippe Champagne, Ministre canadien de l'Innovation, des Sciences et de l'Industrie a pris la parole pendant l'incident pour rappeler l'importance capitale des télécommunications pour les canadiens.[3] Par la suite, Rogers Communication a du rendre compte à l'autorité canadienne compétente (Canadian Radio-television and Telecommunications Commission).

Vers des réseaux "supercritiques" Les nouveaux usages envisagés dans le contexte de la 5G et rappelés lors de débat parlementaire de la loi dite 5G [23] [41] vont augmenter le besoin en disponibilité. Par exemple, l'Etat a confirmé son intérêt pour compléter/remplacer les réseaux régaliens historiques dédiés de type TETRAPOL (Rubis pour la Gendarmerie, Acropol pour la Police, Antarès pour les services d'incendie et de secours) par des réseaux privés prioritaires sur les réseaux civils à l'image du projet du Ministère de l'Intérieur RRF - Réseau Radio du Futur [29]. Un autre usage possible concerne l'utilisation de la 5G comme moyen de communication interne des opérateurs des SAIV - Secteur d'Activité d'Importance Vitale - [28] comme l'industrie (le terme "industrie 4.0" revient régulièrement), la santé (télé-médecine, réseau interne des établissements de santé), les transports, l'énergie, etc. Cela signifie que désormais, les attendus au niveau disponibilité et intégrité deviennent primordiaux. Le terme de réseaux "supercritiques" est même utilisé [23].

5.2 Contexte géopolitique

Des opérations de renseignement Les réseaux mobiles gèrent plusieurs données qui intéressent particulièrement les services de renseignement : localisalisation des UE, compte-rendu des appels passés par les UE, interception des communications électroniques d'un UE, etc. Les services de renseignement n'hésitent pas à lancer des opérations complexes pour s'infiltrer dans les réseaux des opérateurs de communications électroniques et capter des données concernant les UE ciblés. Trois exemples d'opérations de renseignement extérieur rendus publics sont présentés ci-dessous. Ils

[3] `https://twitter.com/fp_champagne/status/1545432860215091200`

ont contribué à faire progresser le niveau de sécurité des opérateurs de communications électroniques, y compris en matière d'exploitation des réseaux mobiles. Ils ont indirectement participé à l'évolution des législations afin de protéger les données personnelles et le secret des correspondances (voir section 5.4 relative à l'évolution réglementaire).

2004 : Compromission d'un cœur de réseau mobile à des fin d'espionnage Les équipements Ericsson AXE déployés par Vodafone Greece disposaient dès 2002 d'un module implémentant des fonctions d'interception. Ce module a été modifié en 2004 afin de permettre l'interception illégale d'une centaine de numéros de téléphone, à commencer par celui du premier ministre grec. La méthode utilisée pour introduire ce code malveillant et pour mettre à jour la liste des numéros illégalement interceptés n'a pas été rendu publique, mais l'organisme de contrôle grec qui a enquêté (AΔAE) évoque une possible implication de personnels d'Ericsson et/ou de personnels de Vodafone [42] en lien avec les services de renseignement américains [68]. Des documents classifiés publiés par Snowden en 2012 mentionnent explicitement des opérations menés par les services de renseignement américains en Grèce à l'occasion des Jeux Olympiques de 2004, en lien avec les services de renseignement grecs [66]. Cet incident pose plusieurs questions plus que jamais d'actualité :

— Comment assurer la sécurité des accès en administration sur les équipements réseaux ?
— Comment garantir l'intégrité des logiciels ? (et s'assurer que les mécanismes de contrôle d'intégrité ne peuvent pas être contournés).
— Comment s'assurer de l'intégrité du personnel des opérateurs ?

2010 : SIGINT AURORAGOLD Plusieurs documents révélés par Snowden en 2012 mettent en avant l'attention particulière des services renseignements vis à vis des opérateurs mobiles [40]. Ils appliquent une collecte d'information en amont d'opérations de renseignement extérieures, notamment les informations techniques échangées entre opérateurs (IR.21) pour permettre le roaming.

2011-2013 : Opération "Socialist" Après la compromission de Vodafone Greece révélée en 2005, c'est au tour de Belgacom de défrayer la chronique à partir de 2013. Plusieurs éléments publiés [39] [47] [79] convergent sur une opération de renseignement appelée "Operation Socialist" menée par les services de renseignement du Royaume-Uni. Une première étape a permis d'identifier les administrateurs du réseau de Belgacom puis, dans une seconde étape, de compromettre leur poste de travail.

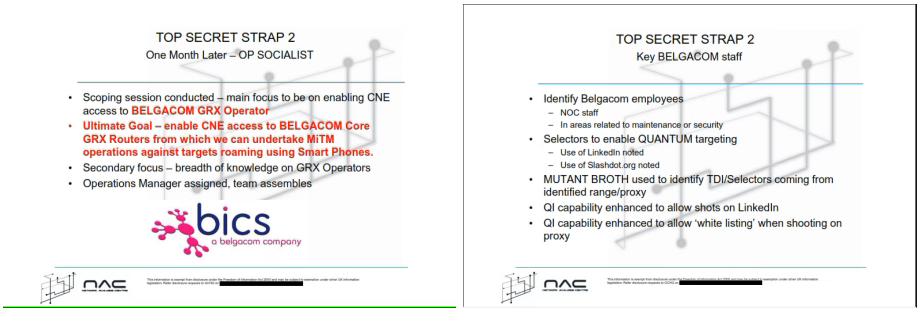

Fig. 22. Opération "Socialist" (source Snowden, `https://nsarchive.gwu.edu/document/22240-document-06-name-redacted-head-gchq-nac`)

Une fois ces postes compromis, une troisième étape a consisté à faire du renseignement sur la topologie du réseau de Belgacom et sur les login/mot de passe utilisés par les administrateurs pour accéder aux équipements réseaux.

Fig. 23. Opération "Socialist is a success" (source Snowden, `https://nsarchive.gwu.edu/document/22240-document-06-name-redacted-head-gchq-nac`)

Une fois ces éléments maîtrisés, la quatrième étape a consisté à se connecter sur les équipements réseaux pour collecter des données sur les clients jusqu'à ce que Belgacom identifie en 2013 la présence de cette intrusion.

Un nouveau théâtre d'opération militaire Cet intérêt va maintenant au-delà des opérations de renseignement. Le cyberespace est en effet devenu un théâtre d'opération à part entière depuis que les nations développées ont défini des doctrines militaires offensives dans le cyberespace. Les capacités

offensives françaises sont identifiées publiquement en 2018 [55]. La France s'est dotée de doctrines de LIO - Lutte Informatique Offensive (LIO) en 2019.[4] La France prévoit un renforcement de ses capacités offensives d'ici 2030 [61]. Des opérations militaires impactant les opérateurs réseaux sont désormais une réalité à l'image de l'attaque du réseau KA-SAT. En effet, le 24 février 2022, vers 3h UTC, alors que l'opération militaire "spéciale" menée par l'armée russe débutait en Ukraine, l'opérateur satellite Viasat a été visée par une attaque : elle a consisté en une compromission d'un accès en administration puis en un dénis de service ciblant les modems utilisés sur les services SurfBeam2 et SurfBeam 2+ de KA-SAT en Europe, en particulier en Ukraine. Les modems ont été "grillés" à savoir que leur firmware ont été modifés de sorte qu'ils ne pouvaient plus avoir accès au service satellite KA-SAT [80] [30].

Une question de souveraineté Un autre angle d'analyse concerne les tensions entre les US et l'Europe d'un côté et la Chine de l'autre. Elles portent sur des questions de dépendances technologiques, d'enjeux économiques et, finalement, sur des questions de souveraineté. Ce contexte géopolitique impacte les choix opérationnels des opérateurs. Côté américain, il est possible de citer comme exemple l'interdiction de la vente d'équipements réseau chinois sur le territoire américain [5] et l'interdiction d'exporter vers la Chine des technologies identifiées comme sensibles. En France, la loi 5G [58] s'inscrit aussi dans ce contexte. Cet article y reviendra dans la section 5.4 relative à l'évolution réglementaire.

5.3 Marché opérateurs

Dans le contexte de la 1G, les opérateurs, souvent les opérateurs historiques publics (Deutsche Telekom, British Telecom, Telecom Italia, etc.) et en nombre limité, constituaient un cercle considéré comme "de confiance". Ce cercle des opérateurs mobiles s'est progressivement étendu à la fin du XX$^{\text{ème}}$ siècle avec la libéralisation des marchés à un nombre beaucoup plus important d'acteurs, voyant apparaitre des opérateurs "gris" : d'un côté, ils opèrent des réseaux mobiles et à ce titre se connectent avec les autres opérateurs en SS7/Diameter, de l'autre côté, ils offrent l'accès payant à des interfaces permettant à des tiers malveillants de réaliser des requêtes SS7 sans ce soucier de leur légitimité. D'autres opérateurs, qui

[4] `https://www.defense.gouv.fr/nos-expertises/cyberdefense-au-ministere-armees`

[5] `https://en.wikipedia.org/wiki/China-United_States_trade_war`

consacrent peu de moyens à leur sécurité, sont des cibles faciles pour des acteurs malveillants qui piratent tout ou partie de leurs réseaux mobiles et s'en servent pour mener à bien discrètement leurs opérations illicites comme des opérations de renseignement ou du détournement de SMS utilisés pour de l'authentification de type 2FA - Two-Factor Authentication.

5.4 Évolution réglementaire

Le contexte réglementaire en France ne cesse de se renforcer, souvent en lien étroit avec le contexte réglementaire européen [49]. Sans rentrer dans le détail, il est possible de citer plusieurs axes qui concernent directement les opérateurs mobiles.

Sécurité des réseaux Il s'agit d'une obligation réglementaire historique identifiée dans les articles L33-1, D98-4 et D98-5 du CPCE - Code des Postes et des Communications Électroniques [59]. De plus, depuis 2011 et l'ajout de l'article L33-10 dans le CPCE [51], le Ministre chargé des communications électroniques peut imposer à tout opérateur de soumettre ses réseaux à un contrôle de sécurité. Il y a eu depuis plusieurs contrôles réalisés, voir par exemple [25].

Protection des données personnelles La loi informatique et libertés de 1978 [50] a longtemps été une référence au-delà des frontières nationales. Elle a fait l'objet d'une mise à jour en 2018 [54] afin de prendre en compte le nouveau RGPD - Règlement Général sur la Protection des Données - établi au niveau européen en 2016. Sur le périmètre de l'opérateur réseau mobile, il est possible de citer comme données personnelles l'IMSI, le MSISDN, la localisation du client ou encore les compte-rendus d'appels voix (qui appelle qui à quelle heure).

Le secret des correspondances L'article 226-3 du code pénal [60] traite de l'atteinte à la vie privée. Est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à nuire au secret des correspondances y compris par négligence, en l'absence d'autorisation ministérielle prévu à l'article R.226-3 et à l'article R.226-7 du code pénal. Le périmètre des équipements concernés a été étendu en 2013 (article 23 de la loi de programmation militaire 2014-2019 [52]). La plupart des équipements du cœur de réseau mobile sont soumis à ce régime d'autorisation administrative. L'article

226-15 du code pénal traite lui spécifiquement de l'atteinte au secret des correspondances. Le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.

Souveraineté nationale Il convient de rappeler que le secteur des communications électroniques est identifié comme un SAIV - Secteur d'Activité d'Importance Vitale [28]. Pour reprendre les propos d'un parlementaire [23] "on peut estimer que les principaux opérateurs de télécommunication, et notamment ceux exploitant des réseaux radioélectriques mobiles, figurent parmi ces OIV - Opérateur d'Importance Vitale. Les bases des SIIV - Système d'Information d'Importance Vitale - ont été posées dans la loi de programmation militaire 2014-2019 (article 21 et suivants, voir [52]) et dans un arrêté de 2016 fixant les règles et les modalités pour le secteur d'activité des communications électroniques [53]. En 2019, la loi n°2019-810 [58], dite loi "5G", a été promulguée, ajoutant des contraintes complémentaires aux opérateurs. Elle vise à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux mobiles. Un décret précise les modalités [57] et un arrêté fixe la liste des appareils prévus [56]. Deux éléments sont marquants. Le premier concerne la liste des équipements. Les gNodeB sont concernés par ces autorisations administratives alors quelles ne sont pas concernées par les autorisations prévues dans les articles R.226-3/-7 du code pénal. Le second concerne le contenu des demandes d'autorisation qui doivent inclure :

- L'objet, la dénomination, la ou les versions et les caractéristiques techniques de l'appareil, accompagnés de la documentation technique de l'appareil fournie par son fabricant ;
- L'utilisation prévue de l'appareil au sein du réseau de l'opérateur ;
- Les modalités de déploiement de l'appareil, précisant l'activation ou la non-activation des fonctionnalités optionnelles de celui-ci, les modalités de protection adoptées pour ses interconnexions avec d'autres éléments du réseau et les logiciels informatiques non spécialisés, systèmes d'exploitation et éventuelles solutions de virtualisation sur lesquels repose l'hébergement informatique de l'appareil et de ses données, les modalités de sécurisation de ces logiciels, ainsi que l'éventuel hébergement de l'appareil avec d'autres appareils sur une même infrastructure informatique ;

— Les modalités d'exploitation de l'appareil, précisant les opérations de configuration, de supervision et de maintenance susceptibles d'être réalisées en cours de fonctionnement ou sur l'hébergement informatique, ainsi que les sous-traitants réalisant des opérations de configuration, de supervision ou de maintenance sur l'appareil.

Le Premier ministre refuse l'octroi de l'autorisation s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale résultant du manque de garantie du respect des règles mentionnées relatives à la permanence, à l'intégrité, à la sécurité, à la disponibilité du réseau, ou à la confidentialité des messages transmis et des informations liées aux communications. Le Premier ministre prend en considération, pour l'appréciation de ce risque, le niveau de sécurité des appareils, leurs modalités de déploiement et d'exploitation envisagées par l'opérateur et le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un Etat non membre de l'Union européenne.

Directive NIS2, directive CER et projet de directive CRA La directive NIS2 - Network and Information Security 2 - [34] et la directive CER - Critical Entities Resilience - [35] ont été approuvées le 14 décembre 2022. Elles devront être transposées et entrer en application dans le droit français avant le 18 octobre 2024.

NIS2 La cybersécurité est traitée dans la directive NIS2. Elle définit des entités "essentielles" qui reprennent dans les grandes lignes les SAIV définies en France [28]. Parmi les entités essentielles identifiées dans la NIS2 figurent les "fournisseurs de réseaux de communications électroniques publics". Elle prévoit, pour les entités essentielles, des règles similaires à celles prévues pour les SIIV en France [53]. Elle ajoute des règles concernant la formation à la sécurité, la gestion du risque, la sécurité de la chaîne d'approvisionnement et l'utilisation de produits et services certifiés. Les sanctions en cas de violations de la directive NIS2 doivent être effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas :

— Amendes administratives d'un montant maximal s'élevant à au moins 10 000 000 EUR ou à au moins 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu ;
— Suspensions temporaires d'autorisations administratives pour l'entité essentielle ou ses dirigeants ;

— Sanctions personnelles pour les dirigeants.

CER L'approche est complémentaire avec la NIS2. La directive CER traite de la sécurité physique et de la sûreté des employés.

CRA - Cyber Resilience Act Une troisième directive est en discussion au niveau européen. Il s'agit de la CRA.[6] Cette future directive traite de l'accès au marché européen des produits numériques. Elle cherche à améliorer le niveau de sécurité de ces produits. Des règles spécifiques concernent des produits critiques comme les équipements de sécurité et les équipements réseau qui ont vocation à intervenir dans la sécurité des entités essentielles définies dans la NIS2. La future directive CRA doit être publiée en 2024 pour une transposition et application au niveau national en 2026.

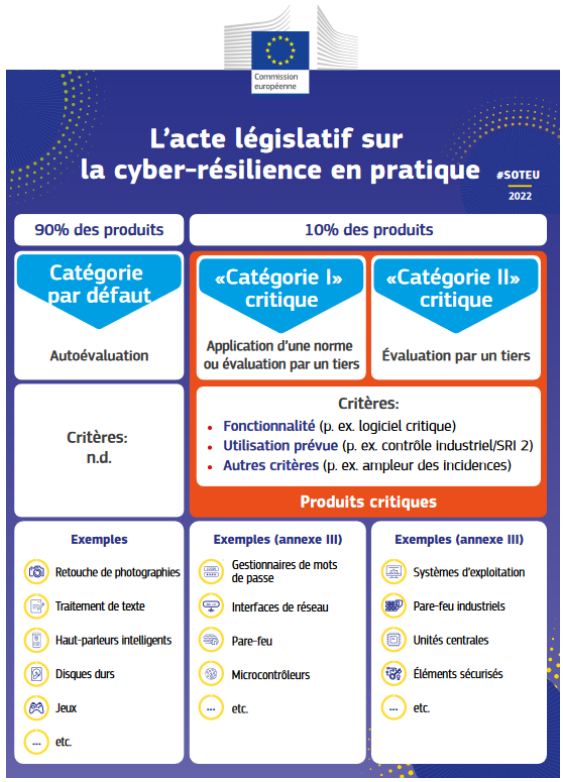

Fig. 24. Cyber Resilience Act, Commission Européenne

[6] https ://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

6 Retour opérationnel sur la sécurité 5G d'un opérateur

L'objectif de cette section est de lever le voile sur un travail collectif sur la sécurité de la 5G, vécu de l'intérieur d'un opérateur. Il s'agit d'une activité au long cours qui a débuté il y a déjà une dizaine d'années par des travaux de recherche. Actuellement la construction du cœur 5G bat son plein chez les opérateurs français. Cette aventure se prolongera dans l'exploitation opérationnelle du réseau 5G et sa déformation quotidienne pour absorber la croissance du trafic, l'amélioration de la sécurité, les mises à jour fonctionnelles et les évolutions des services proposés. Au final, le réseau 5G devrait être opérationnel jusqu'en 2050 en se basant sur la durée de vie du réseau 2G encore en production.

6.1 Travaux de recherche

Les travaux de recherche et d'anticipation sur la 5G ont débuté en 2011-2012 avant le lancement commercial de la 4G en France. Au niveau européen, ils ont pris par exemple la forme du partenariat public-privé (5G-PPP - `https://5g-ppp.eu/`) dans lequel ont été engagés plusieurs acteurs dont les opérateurs. Ces travaux de recherche intègrent dès le début la sécurité avec par exemple dès 2016 le lancement du projet européen "5G Ensure" (`https://www.5gensure.eu/`) et les premières études sur l'architecture et sur la sécurité de la 5G [3]. S'en suivra plusieurs années de productions intenses autour de la sécurité qui alimenteront les travaux en normalisation, notamment le groupe de travail SA3 du 3GPP dédié aux questions de sécurité. Le groupe de travail SA3 a ainsi produit le document "Architecture et procédures de sécurité pour le système 5G" [22].

6.2 Démarche sécurité intégrée à toutes les phases du programme 5G

La sécurité a été intégrée dans la création du programme dédié à la construction du futur réseau 5G d'Orange France et le sera dans toutes les phases opérationnelles.

Politique de sécurité Lors de la spécification du futur réseau 5G d'Orange France, une politique de sécurité dédiée a été rédigée et publiée en interne du programme 5G en 2021. Elle s'inspire de la méthodologie EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité - développée par l'ANSSI. Après avoir défini son périmètre, cette politique

de sécurité explicite les objectifs de sécurité à atteindre sous l'angle réglementaire, normatif ou encore en matière de besoin de sécurité. Une représentation gigogne des enjeux sécurité pourrait être la suivante :

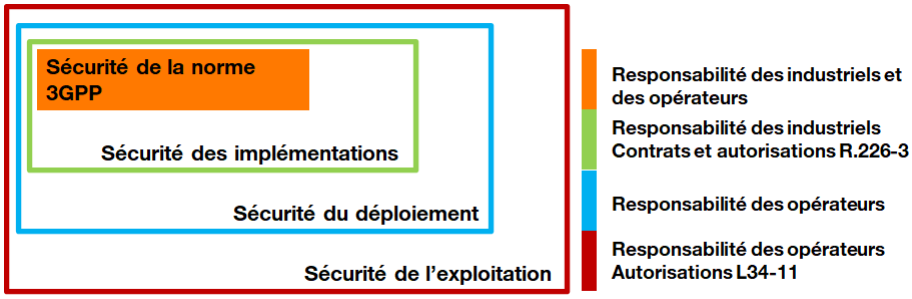

Fig. 25. Représentation gigogne des enjeux sécurité en 5G

Les industriels et les opérateurs travaillent en normalisation pour spécifier les mécanismes de sécurité. Les industriels font alors des choix d'implémentation, y compris vis à vis des options proposées par les normes. Lors de la construction du réseau par l'opérateur à partir de ces briques fournies par les industriels, interviendrait alors la sécurité lors de l'intégration et le déploiement du réseau, dont la responsabilité revient à l'opérateur. L'opérateur fait alors des choix de configuration. Le tout est englobé dans la sécurité de l'exploitation du service rendu au client qui est, comme l'a bien identifié le législateur dans le contexte de la loi dite 5G [58], de la responsabilité de l'opérateur. Elle explicite ensuite les règles de sécurité, tant au niveau technique que non technique (organisationnel ou juridique), qui vont servir de cibles à atteindre pour le programme 5G d'Orange France. Cette démarche a de plus permis d'identifier des chantiers spécifiques à lancer en amont de la construction du réseau 5G comme la création d'une zone d'administration avec un niveau renforcé de sécurité, l'évolution de l'urbanisme des VPNs ou encore une évolution importante de l'infrastructure de gestion de clés publiques (PKI) interne au groupe Orange afin de pouvoir répondre au besoin omniprésent de certificats (tunnels IPSec, interfaces d'administration, SBI - Service-Based Interface - avec le chiffrement activé) dans un réseau 5G.

Formation des personnels : un feu d'artifice La 5G amène un changement radical dans la façon de construire et d'opérer un réseau mobile. En effet, la 5G a été spécifiée comme étant composée d'une multitude de

fonctions réseaux sous forme de logiciels interagissant ensemble via des services web. Ces interactions reposent sur un bus de signalisation SBI basé sur le protocole http/2 avec un enrichissement des en-têtes spécifié par le 3GPP. De plus, la démarche engagée par l'industrie et par les opérateurs amène à se tourner naturellement vers des solutions virtualisées (IaaS - Infrastructure-as-a-Service - ou CaaS - Containers as a Service) pour héberger les fonctions réseaux et à une automatisation des tâches de production et d'exploitation des réseaux. A mi-chemin entre la technique et l'organisationnelle, des démarches de type projet Agile et intégration continue/développement et déploiement continue (CI/CD) sont également mises en oeuvre. Cela oblige bien sûr à revoir complètement la façon d'aborder la sécurité et à développer de nouvelles compétences en matière de sécurité au sein des opérateurs. Un exemple de ces nouveaux métiers peut être le métier d'ingénieur "DevSecOps". Il s'agit aussi d'opportunités pour développer une sécurité au plus proche des fonctions réseaux, en automatisant des contrôles de cohérence par rapport à des configurations de référence ou en réalisant des tests de sécurité, en étant plus agile dans le déploiement de mise à jour de sécurité ou encore en générant des inventaires à jour des différents composants déployés. Pour terminer ce feu d'artifice, il est difficile de ne pas parler de l'IA - Intelligence Artificielle - de façon générique. L'IA commence à être utilisée dans les réseaux des opérateurs afin par exemple d'optimiser le fonctionnement du RAN, afin de détecter des évènements anormaux en termes de supervision ou encore afin de détecter des signaux faibles permettant de prévenir des pannes en réalisant des opérations de maintenance préventive. Comme toute nouvelle technologie, elle nécessite aussi de prendre du recul au niveau de la sécurité. L'IA peut générer un résultat biaisé qui, lorsqu'il génère des actions automatisées, peut avoir des impacts opérationnels immédiats. Là encore des compétences spécifiques en matière de sécurité appliquée au domaine de l'IA ont été développées au sein des opérateurs.

Appel d'offre Plusieurs appels d'offres ont été lancés pour couvrir l'ensemble des segments du réseau 5G dès 2018. A chaque appel d'offre, des exigences sécurité et réglementaires ont été intégrées. Les exigences sécurité se basent principalement sur le standard 3GPP, sur les recommandations de l'ANSSI ou sur des standards industriels reconnus des fournisseurs retenus. Les exigences réglementaires ont par exemple porté sur les autorisations R.226-3 (au sens du code pénal) lorsque nécessaire. Outre le cahier des charges initial et l'analyse des réponses apportées, des oraux dédiés à la sécurité ont été organisés sur différentes thématiques comme la sécurité

du socle de virtualisation proposé, le durcissement des produits ou encore sur les protocoles sécurisés mis en œuvre sur les différents plans.

Contractualisation Les contrats intègrent systématiquement des clauses spécifiques pour d'une part s'engager dans le respect du RGPD et d'autre part s'engager sur une approche vertueuse de la sécurité. Pour ce dernier point, outre les attendus en matière d'intégration native de la sécurité des produits, il est également demandé un engagement de correction des vulnérabilités identifiées dans un délais fixé qui dépend du niveau de gravité de la vulnérabilité.

Tests fonctionnels de sécurité en laboratoire Les tests fonctionnels en laboratoire sont un passage obligé dans le processus de mise en œuvre d'un réseau. Ils répondent dans un premier temps à un besoin d'évaluation puis dans un second, à un principe de qualification ou validation. L'évaluation d'une plate-forme, d'un produit ou d'un service s'exerce durant des phases amonts de veille technologique ou plus tard lors d'appel d'offre. Cette étape permet alors des choix éclairés sur la base de résultats concrets et d'une mise en œuvre pratique des fonctions de sécurité. En effet, cette dernière est souvent le parent pauvre de certains systèmes, il est ainsi plus aisé de contrôler l'effort consenti par un constructeur dans ce domaine.
L'étape de validation répond à un besoin différent, il s'agit pour l'opérateur de vérifier le bon fonctionnement de l'ensemble des fonctions de sécurité du système sous test et de leur bonne adéquation avec l'écosystème dans lequel il sera intégré. Cette étape importante porte sur l'ensemble des besoins de sécurité. Elle couvre les interactions entre le terminal mobile et le réseau de l'opérateur (authentification, chiffrement RAN), les interactions entre les fonctions en interne du réseau mais aussi les cas d'itinérance auxquelles s'ajoute la protection globale de l'infrastructure comme, par exemple, le contrôle des accès (application de gestion des équipements, accès distant aux systèmes...).
Les réseaux 5G s'appuient sur de nombreux protocoles dont certains intègrent leur propre mécanisme de sécurité et pour d'autres sont protégés par l'ajout de fonctions dédiées. Chacun de ces mécanismes nécessite d'être vérifié. Le respect protocolaire, souvent sujet à interprétation, des fonctions liées à la 5G (fonctionnement et présence conformes aux spécifications), leur interopérabilité avec leur environnement sont autant d'éléments à contrôler.
Les réseaux mobiles ont toujours été des systèmes complexes. Si les plates-formes étaient plutôt monolithiques dans les générations précédentes, le

marché de la 4G a déjà introduit la virtualisation. La 5G a ensuite poussé encore plus loin ce principe d'éclatement des fonctions du réseau. La technologie sous-jacente s'appuie maintenant sur la notion de conteneur. Chaque étape de ces progrès a eu un effet multiplicateur sur le nombre d'éléments de sécurité à vérifier par l'introduction de nouvelles couches dont les contrôles se sont vus ajouter à ceux réalisés précédemment. Ainsi, de par le nombre croissant de serveurs, de machines virtuelles, de couches logicielles et de leur dépendance, l'automatisation est devenue un objectif incontournable, accentuée par des cycles de livraison et de mise œuvre bien plus rapide. De ce fait, les tests fonctionnels de sécurité rentrent maintenant dans un modèle classique du développement logiciel avec une multitude de tests lancée régulièrement et complétée par une série d'opérations de contrôle manuel pour lesquels les développements ne seraient pas opportuns. Néanmoins, cette automatisation soulève quelques difficultés. En particulier, les outils automatisés génèrent un nombre important de faux positifs dans l'analyse des CVE. Leur traitement manuel devient alors conséquent. En outre, comme aucune solution ou produit n'est jamais parfait, il devient indispensable de fixer le seuil d'acceptation de la criticité des CVE acceptés.
La 5G apporte son lot d'amélioration en sécurité, notamment en cœur de réseau. Le bus de communication interne (SBI) est par exemple naturellement protégé par mTLS. Cette protection n'est pas sans conséquence pour un contrôle efficace du fonctionnement de la signalisation du réseau mobile. En effet, cette analyse protocolaire par des sondes dédiées devient impossible, il est alors requis de passer par les équipements 5G eux-mêmes pour une investigation qui devient de ce fait moins indépendante.

6.3 Security by design

Cette section illustre quelques choix réalisés par Orange France sans rechercher l'exhaustivité.

Activation des fonctions sécurité prévues par le 3GPP

Chiffrement et filtrage entre RAN et cœur 5G Fort de l'expérience acquise en 4G depuis 2012, des tunnels IPsec sont systématiquement montés entre les eNodeB (4G) ou les gNodeB (5G) côté RAN et des SEG - Security Gateway - côté cœur de réseau. Les SEG sont non seulement point de terminaison IPsec mais assurent aussi un rôle important dans le filtrage des flux entre le RAN (domaine non sûr) et le cœur de réseau 5G

(domaine sûr). Au-delà des aspects sécurité pour la 4G et la 5G, il s'agit d'un challenge opérationnel pour l'opérateur en termes de volumétrie de tunnels (environ 100 000 tunnels qui évoluent quotidiennement au gré de la production de sites RAN), en termes de trafic client (l'ordre de grandeur est le Tb/s de trafic cumulé en pointe, en croissance permanente) et en termes d'expérience client (limiter par exemple la latence ou limiter l'impact de la défaillance d'un équipement). Ces volumétries combinées aux fonctions de sécurité activées amènent périodiquement à approcher les limites techniques capacitaires des SEG et à devoir procéder à des mises à jour de matériel.

Chiffrement du bus SBI portant la signalisation du cœur 5G La démarche peut surprendre de premier abord, et n'est pas forcément naturelle pour celles et ceux qui ont déjà mis les mains dans le "cambouis". Activer d'emblée les fonctions de sécurité, notamment le chiffrement des flux, entraîne une difficulté dans l'intégration des différents composants puisque un TCPDump et un Wireshark ne servent plus à rien. Il n'est plus possible d'observer les échanges entre les applications afin de vérifier leur conformité protocolaire. Il faut s'en remettre aux logs. Ce choix oblige une plus grande rigueur dans la configuration des applications et dans les tests d'intégration. Il faut de plus redoubler d'effort pour comprendre l'implémentation des normes par les industriels retenus. Pourtant, Orange France a fait le pari d'activer dès le début le chiffrement sur toutes les interfaces, typiquement sur le bus de signalisation SBI et force de constater que ce choix a été très instructif d'un point de vue opérationnel. Il a permis de travailler avec les industriels afin de répondre aux besoins des exploitants en matière de log, d'identifier des erreurs d'implémentation dans la gestion des clés et des certificats ou encore de faire évoluer les logiciels afin d'intégrer des protocoles à jour et un sous-ensemble commun de suites cryptographiques conforme à l'état de l'art. A contrario, l'expérience de terrain montre que lorsque le chiffrement n'est pas activé de suite, son activation peut s'avérer douloureuse en raison du risque d'incident et de l'impact sur les procédures d'exploitation.

Chaîne d'exploitation Un effort significatif a porté sur une refonte de la chaîne d'exploitation, intégrant nativement la notion d'accès "humain" et la notion d'accès "machine". Le premier, l'accès "humain", correspond simplement à l'accès d'un exploitant depuis un poste d'administration. Le second, l'accès "machine" englobe toutes les actions lancées depuis une machine ou un logiciel pour exploiter le réseau 5G. Il est possible

d'y inclure notamment les scripts d'automatisation lancés potentiellement depuis un GitLab interne. Un effort significatif a été mis sur la sécurisation du poste d'administration et sur un bastion en coupure entre le poste d'administration et les ressources à administrer. Ce bastion gère d'une façon atypique mais performante et sécurisée la diversité des flux d'administration :

- L'utilisateur s'authentifie avec une solution interne à 2 facteurs forts en arrivant sur un portail. Une fois authentifié, il voit sur ce portail l'ensemble des ressources qu'il peut joindre au regard de ses droits et il n'a plus qu'à "cliquer" sur la ressource qui l'intéresse sans avoir besoin de s'authentifier à nouveau sur la cible pour lancer une console ou une fenêtre web.
- Le bastion distingue d'une part les flux de type ligne de commande (ex : connexion ssh sur une ressource) et les flux de type web (ex : accès au GitLab ou accès à un gestionnaire) afin de proposer des chaînes techniques adaptées.

Outre le bastion, une nouvelle zone d'administration dédiée au réseau mobile a été crée. Elle est composée de plusieurs sous-zones distinctes, à même d'héberger des outils ayant des besoins de sécurité différents. Ces zones disposent d'espace en baie pour héberger des serveurs physiques et proposent par ailleurs un socle virtualisé avec des ressources disponibles pour instancier des VMs en fonction des besoins des exploitants. Cette zone héberge aussi tous les outils nécessaires comme des relais NTP, des serveurs DNS (un domaine DNS spécifique au réseau mobile a été alloué), les serveurs nécessaires au bon fonctionnement de la PKI, les serveurs de log, etc. Le tout fonctionne en IPv4 et en IPv6.

Durcissement à tous les étages

Socle système Les bonnes pratiques en matière de durcissement des systèmes d'exploitation sont mises en oeuvre, en lien étroit avec les fournisseurs retenus des fonctions réseaux.

Cloud privé Plusieurs Clouds privés sont en cours d'assemblage pour assurer la disponibilité du coeur 5G de production. Ils mettent en oeuvre un niveau renforcé de sécurité, avec notamment l'usage de HSM - Hardware Security Module -, de mécanismes d'isolation réseau et l'usage systématique de protocoles sécurisés pour l'administration des Clouds.

Applications L'opérateur a peu de leviers sur l'application à proprement parler, hormis les fonctions mises à disposition par le fournisseur. Un

travail de configuration est prévu pour chaque application afin de trouver les meilleurs compromis en termes de sécurité. Un exemple des choix réalisés par Orange France concerne la mise en œuvre de HSM dédiés à la fonction 5G ARPF pour sécuriser l'accès aux K_i et générer les vecteurs d'authentification.

Automatisation L'automatisation est perçue comme un atout indispensable pour la mise en oeuvre d'un coeur 5G. Il permet le déploiement de configurations homogènes respectant des patterns pré-définis. L'automatisation permet de vérifier la conformité des configuration en production par rapport à ces patterns et de maintenir des référentiels à jour du parc de logiciel déployé. De plus, l'automatisation permet d'auditer les scripts ou des applications pour s'assurer du respect des règles de sécurité, avant leur déploiement en production. La contrepartie est qu'il est nécessaire de consacrer du temps et des ressources en amont dans l'automatisation pour écrire/intégrer/tester les scripts, y compris les scripts de sécurité.

Analyse de risque et audit - une approche complémentaire

Analyse de risque L'analyse de risque est un principe incontournable pour une organisation dans le domaine de la cybersécurité. Elle permet de cartographier l'ensemble des risques cyber, stratégiques, juridiques, financiers et de ressources pour un système donné et par conséquence permet de construire une politique de sécurité adaptée.
Plusieurs analyses de risque ont été réalisées dans le contexte de la 5G. Une première analyse globale à la technologie 5G puis d'autres études spécifiquement sur chacun des composants réseaux et en particulier sur ceux naturellement exposés : l'AMF (Access Management System) gère l'attachement réseau de l'UE, la NEF (Network Exposure Function) propose la possibilité d'interagir avec le cœur de réseau pour le pilotage de certains terminaux... Ces analyses pointent ainsi les fonctions de sécurité requises pour assurer la protection du réseau 5G, fonctions dont la bonne configuration et le bon fonctionnement pourront être contrôlés lors d'un audit.

Audit L'audit répond à deux besoins, celui d'une recette des fonctions de sécurité avant mise en production, puis celui d'un contrôle à une étape ultérieure dans le cycle de vie du réseau mobile. Dans les deux cas, la définition d'un périmètre d'étude est un préalable, allant potentiellement de l'accès radio aux réseaux d'interconnexion entre opérateurs.
Tout comme pour les tests fonctionnels, les technologies des fonctions de

sécurité autour de la 5G évoluent beaucoup. Ainsi, s'appuyant sur Kubernetes, les plates-formes suivent l'évolution rapide de cet environnement. Par principe, cette évolution concerne aussi les fonctions et mécanismes de sécurité. Ceci devient un défi pour les constructeurs de ne pas proposer des solutions qui seront rapidement caduques mais il convient aussi de maîtriser ces mécanismes pour en assurer la bonne mise en œuvre et un contrôle effectif.

Et le bug Bounty ? Impensable il y a encore une dizaine d'année, Orange France s'est lancé dans le bain en 2016 lors de la nuit du hack en ciblant le service d'annuaire "118712.fr".[7] Depuis, Orange France organise régulièrement des programmes de Bug Bounty publics ou privés, ciblant principalement les services Web exposés sur Internet. Le lancement d'un Bug Bounty sur un sous-périmètre du réseau 5G n'est pas exclu dans le futur.

Supervision sécurité La supervision en général du cœur 5G, et la supervision sécurité en particulier vont être un défi à part entière au regard du volume de log qu'il est potentiellement possible de remonter au niveau de l'infra support, au niveau système ou encore au niveau applicatif. Un ou plusieurs niveau d'agrégation de log vont être nécessaires pour ne remonter vers la supervision sécurité que les logs pertinent au regard des scénarios de menace envisagés dans les analyses de risques.

6.4 Prise de recule sur la sécurité 5G (partie à compléter)

Fausses stations de base

Côté opérateur Le sujet est problématique, mais le bout du tunnel approche pour plusieurs raisons. D'abord, les opérateurs arrêtent progressivement la 2G et la 3G. Concernant Orange France, l'extinction est prévue en 2025 pour la 2G et en 2028 pour la 3G. [64]. Reste la 4G où l'IMSI est envoyée en clair sur le RAN dans certaines circonstances avant de basculer sur une identité temporaire. Concernant la 5G-SA, les premiers retours sont plutôt positifs dès lors que le réseau est correctement configuré pour utiliser les SUCI, voir par exemple [24].

[7] `https://www.orange-business.com/fr/blogs/securite/actualites/bug-bounty-nuit-du-hack-2017-orange-un-an-apres`

Côté terminaux La désactivation de la 2G/3G au niveau des opérateurs réseaux n'est cependant pas suffisante si les terminaux autorisent toujours les connexions en 2G/3G sur des fausses stations de base. Les constructeurs commencent à implémenter au niveau des terminaux des fonctions permettant de désactiver la 2G/3G. Android 12 a ouvert la voix à la désactivation de la 2G ([69]). Mais le mode opératoire pour cette désactivation n'est pas trivial et reste réservé à un public averti. De plus, cela ne concerne que la 2G (et pas la 3G ou la 4G). Enfin, cela reste un cas isolé puisque des acteurs comme Apple, Huawei ou Samsung n'offrent pas de fonctionnalités similaires. Pour l'instant.

Augmentation de la surface exposée Si historiquement les opérateurs mettaient en oeuvre des protocoles "telco" sur des équipements dédiés que peu de personnes connaissaient, il y avait une forme de sécurité par l'obscurantisme. Ce n'est clairement plus le cas en 5G SA. En normalisation, la 3GPP a résolument fait le choix d'utiliser des protocoles "sur étagère" : réseau tout "IP", usage de protocoles comme IPsec ou http/2, algo de chiffrement éprouvés comme AES, etc. Par ailleurs, les fournisseurs de fonctions 5G développent désormais des logiciels en se basant sur des composants/bibliothèques/OS connus. Ces choix permettent de gagner du temps et de reposer sur des solutions éprouvées. Mais ils augmentent le nombre d'acteurs qui peuvent chercher des vulnérabilités et indirectement exposent les produits en cas de failles avérés. Cela oblige donc à être plus réactifs dans l'intégration des correctifs chez les fournisseurs, dans les tests de non régression et dans le déploiement opérationnel. Un exemple qui a marqué les esprits est l'usage de la bibliothèque "log4J" et les failles associées publiées fin 2021. Outre cet aspect, les opérateurs intègrent également l'augmentation de la surface d'attaque liée à la mise en oeuvre de nouvelles pratiques (agilité, automatisation, etc.) et de nouvelles technologies (virtualisation, services web, etc.). Un prérequis est ici d'intégrer ce nouveau paradigme dans l'approche globale de la sécurité. Il ne sert à rien de durcir une fonction 5G si la chaîne CI/CD, qui intervient dans la mise à jour de cette fonction, n'est pas également sécurisée.

7 Perspectives

7.1 6G à horizon 2030

Les travaux exploratoires autour de la 6G ont débuté. Ils devraient se conclure en 2025 par la définition des principaux objectifs de la 6G. Deux

orientations sont possibles à ce stade. Reprendre les travaux sur la base de la spécification de la 5G et apporter des évolutions ou privilégier un scénario en rupture pour la 6G. Les travaux en normalisation à 3GPP devraient débuter en 2025 et cibler une première version stable des spécifications de la 6G à horizon 2030. Cela amènerait à une ouverture commerciale en 2031-2032, le temps de déployer les réseaux et le temps que les premiers terminaux compatibles soient commercialisés.

7.2 Cryptographie post-quantique à tous les étages

Sous l'angle de la sécurité, la principale thématique qui doit être traitée porte sur la cryptographie post-quantique, notamment pour les fonctions reposants sur les algorithmes de cryptographie asymétrique : SBA (PKI, http/2), négociation des clés utilisées pour monter les tunnels IPsec et mécanisme d'anonymisation (SUPI/SUCI) vont devoir être retravaillés pour être résiliant à la cryptanalyse utilisant des ordinateurs quantique. La cryptographie symétrique va devoir passer sur des tailles de clé à 256 bits (travaux en cours au 3GPP).

7.3 Évolutions

Plusieurs évolutions sont d'ores et déjà envisagées. L'architecture SBA va tout d'abord être retravaillée/améliorée pour être plus efficace et plus cloud native. Ensuite, la question de l'intégration de l'IA dans les réseaux mobiles va être plus prégnante pour améliorer l'expérience utilisateur et optimiser le fonctionnement des réseaux. De plus, les réflexions vont porter sur une meilleur intégration des réseaux avec les infrastructures virtualisées (cloud public/cloud privé, mixte) en intégrant les nouveaux paradigmes permis par la virtualisation et l'automatisation introduits en 5G. Enfin, il est probable que des enjeux environnementaux soient intégrés à tous les niveaux de la 6G, y compris au niveau de la sécurité, afin d'avoir une approche plus vertueuse.

8 Conclusion

Au cours des dernières décennies, la sécurité d'un réseau mobile est devenue un sujet de plus en plus complexe techniquement et de plus en plus critique stratégiquement afin de répondre aux attentes croissantes des clients. Les travaux en cours dans la construction des futurs réseaux mobiles 5G illustrent la prise en compte de la sécurité à tous les niveaux

avec un engagement fort des opérateurs d'atteindre un niveau de sécurité homogène élevé. Mais ce n'est qu'une étape supplémentaire dans l'histoire des opérateurs qui a débuté au milieu du XX$^{\text{ème}}$ siècle. Au regard de la sensibilité des services rendus par les réseaux mobiles dans les années à venir et au regard de l'appétence d'acteurs malveillants vis à vis de ces mêmes réseaux, il ne fait aucun doute qu'il y aura de nouvelles étapes qui permettront régulièrement de combler les vulnérabilités identifiées et d'améliorer encore le niveau de sécurité du réseau 5G et des réseaux en devenir comme la 6G.

9 Remerciements

En premier lieu, un remerciement sincère à tous les organisateurs du SSTIC qui permettent depuis 20 ans à un large public de monter en compétence dans le domaine de la sécurité. Ensuite, une pensée pour tous les collègues du groupe Orange qui ont contribué directement ou indirectement à cet article : Bérénice Gloria, Stéphane Gorse, Olivier Charles, Emmanuelle Bernard, Sarah Nataf, Todor Gamishev, Irmine Vieira et toute l'équipe sécurité des réseaux d'Orange France.

Références

1. 3GPP. 3gpp ts 21.133 : 3rd generation partnership project ;technical specification group services and system aspects ;3g security ; security threats and requirements (release 4). *3GPP*, 2001. `https://www.3gpp.org/DynaReport/21133`.
2. 3GPP. 3gpp ts 33.120 : 3rd generation partnership project ;technical specification group services and system aspects ;3g security ;security principles and objectives (release 4). *3GPP*, 2001. `https://www.3gpp.org/DynaReport/33120`.
3. 3GPP. 3gpp tsg-sa wg3 meeting 82 ; s3-160278 : Study on architecture and security for next generation system. *3GPP*, 2016. `http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_82_Dubrovnik/docs/S3-160278.zip`.
4. 3GPP. 3gpp ts 23.002 : 3rd generation partnership project ; technical specification group services and system aspects ; network architecture (release 17). *3GPP*, 2021. `https://www.3gpp.org/DynaReport/23002`.
5. 3GPP. 3gpp tr 38.912 : 3rd generation partnership project ; technical specification group radio access network ; study on new radio (nr) access technology (release 17). *3GPP*, 2022. `https://www.3gpp.org/DynaReport/38912`.
6. 3GPP. 3gpp ts 21.102 : 3rd generation partnership project ;technical specification group services and system aspects ;3g security ; security architecture (release 17). *3GPP*, 2022. `https://www.3gpp.org/DynaReport/21102`.
7. 3GPP. 3gpp ts 23.228 : 3rd generation partnership project ;technical specification group services and system aspects ;ip multimedia subsystem (ims) ;stage 2 (release 18). *3GPP*, 2022. `https://www.3gpp.org/DynaReport/23228`.

8. 3GPP. 3gpp ts 23.501 : 3rd generation partnership project ; technical specification group services and system aspects ; system architecture for the 5g system (5gs) ; stage 2 (release 18). *3GPP*, 2022. https://www.3gpp.org/DynaReport/23501.

9. 3GPP. 3gpp ts 23.502 : 3rd generation partnership project ; technical specification group services and system aspects ; procedures for the 5g system (5gs) ; stage 2 (release 18). *3GPP*, 2022. https://www.3gpp.org/DynaReport/23502.

10. 3GPP. 3gpp ts 23.503 : 3rd generation partnership project ; technical specification group services and system aspects ; policy and charging control framework for the 5g system (5gs) ; stage 2 (release 18). *3GPP*, 2022. https://www.3gpp.org/DynaReport/23503.

11. 3GPP. 3gpp ts 29.002 : 3rd generation partnership project ;technical specification group core network and terminals ;mobile application part (map) specification(release 5). *3GPP*, 2022. https://www.3gpp.org/DynaReport/29002.

12. 3GPP. 3gpp ts 29.338 : 3rd generation partnership project ; technical specification group core network and terminals ; diameter based protocols to support short message service (sms) capable mobile management entities (mmes) (release 18). *3GPP*, 2022. https://www.3gpp.org/DynaReport/29338.

13. 3GPP. 3gpp ts 33.210 : 3rd generation partnership project ; technical specification group services and system aspects ; network domain security (nds) ; ip network layer security (release 17). *3GPP*, 2022. https://www.3gpp.org/DynaReport/33210.

14. 3GPP. 3gpp ts 33.310 : 3rd generation partnership project ; technical specification group services and system aspects ; network domain security (nds) ; authentication framework (af) (release 17). *3GPP*, 2022. https://www.3gpp.org/DynaReport/33310.

15. 3GPP. 3gpp ts 33.401 : 3rd generation partnership project ; technical specification group services and system aspects ;3gpp system architecture evolution (sae) ; security architecture (release 17). *3GPP*, 2022. https://www.3gpp.org/DynaReport/33401.

16. 3GPP. 3gpp ts 35.201 : 3rd generation partnership project ; technical specification group services and system aspects ; 3g security ; specification of the 3gpp confidentiality and integrity algorithms ; document 1 : f8 and f9 specification (release 17). *3GPP*, 2022. https://www.3gpp.org/DynaReport/35201.

17. 3GPP. 3gpp ts 35.202 : 3rd generation partnership project ; technical specification group services and system aspects ; 3g security ; specification of the 3gpp confidentiality and integrity algorithms ; document 2 : Kasumi specification (release 17). *3GPP*, 2022. https://www.3gpp.org/DynaReport/35202.

18. 3GPP. 3gpp ts 55.216 : 3rd generation partnership project ; technical specification group services and system aspects ; 3g security ; specification of the a5/3 encryption algorithms for gsm and ecsd, and the gea3 encryption algorithm for gprs ; document 1 : A5/3 and gea3 specifications (release 17). *3GPP*, 2022.

19. 3GPP. 3gpp ts 55.226 : 3rd generation partnership project ; technical specification group services and system aspects ; 3g security ; specification of the a5/4 encryption algorithms for gsm and ecsd, and the gea4 encryption algorithm for gprs (release 17). *3GPP*, 2022.

20. 3GPP. 3gpp ts 23.003 : 3rd generation partnership project ; technical specification group core network and terminals ; numbering, addressing and identification (release 17). *3GPP*, 2023. https://www.3gpp.org/DynaReport/23003.

21. 3GPP. 3gpp ts 33.402 : 3rd generation partnership project ; technical specification group services and system aspects ;3gpp system architecture evolution (sae) ; security aspects of non-3gpp accesses (release 18). *3GPP*, 2023. https://www.3gpp.org/DynaReport/33402.
22. 3GPP. 3gpp ts 33.501 : 3rd generation partnership project ; technical specification group services and system aspects ; security architecture and procedures for 5g system (release 18). *3GPP*, 2023. https://www.3gpp.org/DynaReport/33501.
23. Pascal Allizard. Avis présenté au nom de la commission des affaires étrangères, de la défense et des forces armées sur la proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la france dans le cadre de l'exploitation des réseaux radioélectriques mobiles, 2019. http://www.senat.fr/rap/a18-569/a18-5691.pdf.
24. Ravishankar Borgaonkar and Altaf Shaik. 5g imsi catchers mirage. *BlackHat USA*, 2021. https://www.blackhat.com/us-21/briefings/schedule/#5g-imsi-catchers-mirage-23538.
25. ANSSI IGA IGAS CGE CCED. Evaluation de la gestion par l'opérateur orange de la panne du 2 juin et de ses conséquences sur l'accès aux services d'urgence, 2021. https://www.economie.gouv.fr/files/2021-07/Rapport-Orange-SNU.PDF.
26. Jean Cellmer. Réseaux cellulaires - radiocom 2000. *Techniques de l'Ingénieur*, 1999. https://www.techniques-ingenieur.fr/base-documentaire/archives-th12/archives-reseaux-et-telecommunications-tiate/archive-1/reseaux-cellulaires-e7362/.
27. Marc Cherki, Enguérand Renault, and Marie-Cécile Renault. La panne d'orange devient une affaire d'État. https://www.lefigaro.fr/societes/2012/07/08/20005-20120708ARTFIG00163-la-panne-d-orange-devient-une-affaire-d-etat.php, 2012.
28. SGDSN Secrétariat Général de la Défense et de la Sécurité Nationale. Instruction générale interministérielle relative la sécurité des activités d'importance vitale, n°6600/sgdsn/pse/psn du 7 janvier 2014, 2014. https://www.legifrance.gouv.fr/circulaire/id/37828.
29. Ministère de l'Intérieur et des Outre-mer. Lancement du projet "réseau radio du futur" (rrf), le réseau très haut-débit souverain des services de sécurité et de secours. https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2022-10/13-10-2022-cp-rrf.pdf, 2022.
30. Conseil de l'Union Européenne. Cyberopérations russes contre l'ukraine : déclaration du haut représentant au nom de l'union européenne. https://www.consilium.europa.eu/fr/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/, 2022.
31. Scott D. Easterling, Michael O. Linden, and John C. Voelkel. Multi-channel cellular communications intercept system. https://patents.google.com/patent/US5428667, 1993.
32. Tobias Engel. Locating mobile phones using signalling system #7. *Chaos Communication Congress*, 2008. https://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf.
33. Tobias Engel. Ss7 : Locate. track. manipulate. *Chaos Communication Congress*, 2014. https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf.

34. EUR-Lex. Directive (ue) 2022/2555 du parlement européen et du conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'union, modifiant le règlement (ue) no 910/2014 et la directive (ue) 2018/1972, et abrogeant la directive (ue) 2016/1148 (directive sri 2) (texte présentant de l'intérêt pour l'eee), 2022. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2555.

35. EUR-Lex. Directive (ue) 2022/2557 du parlement européen et du conseil du 14 décembre 2022 concernant sur la résilience des entités critiques, et abrogeant la directive 2008/114/ce du conseil (texte présentant de l'intérêt pour l'eee), 2022. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2557.

36. Dirk Fox. Imsi-catcher. *DuD (Datenschutz und Datensicherheit)*, 1997. https://www.secorvo.de/publikationen/imsi-catcher-fox-1997.pdf.

37. Dirk Fox. Der imsi-catcher. *DuD (Datenschutz und Datensicherheit)*, 2002. https://www.secorvo.de/publikationen/imsicatcher-fox-2002.pdf.

38. Emmanuel Gadaix. Gsm and 3g security. *Black Hat Asia*, 2001. https://www.blackhat.com/presentations/bh-asia-01/gadiax.ppt.

39. Ryan Gallagher. The inside story of how british spies hacked belgium's largest telco. *The Intercept*, 2014. https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/.

40. Ryan Gallagher. Operation auroragold : How the nsa hacks cellphone networks wouldwide. *The Intercept*, 2014. https://theintercept.com/2014/12/04/nsa-auroragold-hack-cellphones/.

41. Thomas Gassiloud. Avis présenté au nom de la commission des affaires étrangères, de la défense et des forces armées sur la proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la france dans le cadre de l'exploitation des réseaux radioélectriques mobiles, 2019. https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b1830_rapport-avis.

42. Kevin Haggerty and Minas Samatas. Surveillance and democracy (see chapter 12. the greek olympic phone tappings scandal : A defenceless state and a weak democracy, minas samatas). *Routledge*, 2010. https://www.ekathimerini.com/in-depth/special-report/202026/americans-and-greeks-started-the-2004-wiretaps-together/#firstPage.

43. Silke Holtmanns, Siddharth Prakash Rao, and Ian Oliver. User location tracking attacks for lte networks using the interworking functionality. *IEEE, IFIP Networking Conference (IFIP Networking)*, 2016.

44. Rogers Communications Inc. Rogers canada-wide service outage of july 2022 - amended abridged rfi responses. https://crtc.gc.ca/otf/eng/2022/8000/c12-202203868.htm, 2022.

45. Hank M. Kluepfel. Securing a global village and its resources : baseline security for interconnected signaling system #7 telecommunications networks. *CCS '93 : Proceedings of the 1st ACM conference on Computer and communications security*, 1993.

46. Dmitry Kurbatov and Kropotov Vladimir. Hacking mobile network via ss7 : interception, shadowing and more - hitcon. *HITCON*, 2015. https://hitcon.org/2015/CMT/download/day1-d-r0.pdf.

47. Kapersky Lab. The regin platform nation-state ownage of gsm networks. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf, 2014.
48. Guillaume Larrivé, Jean-Michel Mis, and Loïc Kevran. Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement. *Assemblée nationale*, 2020. https://www.assemblee-nationale.fr/dyn/15/rapports/micrens/l15b3069_rapport-information.
49. Franck Laurent and Pascal Nourry. Contexte réglementaire pour les opérateurs 5g. *C&ESAR*, 2019. https://www.cesar-conference.org/wp-content/uploads/2019/10/20191119_J1_060_P-NOURRY_Contexte_reglementaire_5G.pdf.
50. Légifrance. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 1978. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000886460.
51. Légifrance. Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, article 6, 2011. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000024502658/.
52. Légifrance. Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, 2013. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028338825/.
53. Légifrance. Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « communications électroniques et internet » et pris en application des articles r. 1332-41-1, r. 1332-41-2 et r. 1332-41-10 du code de la défense, 2016. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033521327?r=LWo2BkmE58.
54. Légifrance. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, 2018. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952/.
55. Légifrance. Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, 2018. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037192797.
56. Légifrance. Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article l. 34-11 du code des postes et des communications électroniques, 2019. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039455672/.
57. Légifrance. Décret n° 2019-1300 du 6 décembre 2019 relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques prévue à l'article l. 34-11 du code des postes et des communications électroniques, 2019. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039455649.
58. Légifrance. Loi n°2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la france dans le cadre de l'exploitation des réseaux radioélectriques mobiles, 2019. https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000038360175/.
59. Légifrance. Code des postes et des communications électroniques, 2023. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070987/.
60. Légifrance. Code pénal, 2023. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719.

61. Légifrance. Projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, 2023. https://www.assemblee-nationale.fr/dyn/16/textes/l16b1033_projet-loi.pdf.

62. Benoit Michau and Marin Moulinier. La signalisation chez les opérateurs mobiles. *SSTIC*, 2022. https://www.sstic.org/2022/presentation/la_signalisation_chez_les_oprateurs_mobiles/.

63. Karsten Nohl. Mobile self-defense. *Chaos Communication Congress*, 2014. https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf.

64. Orange. Orange annonce une nouvelle étape dans la transformation de ses réseaux mobiles en europe, avec l'arrêt progressif des réseaux 2g et 3g avant la fin de la décennie, 2022. https://newsroom.orange.com/orange-annonce-une-nouvelle-etape-dans-la-transformation-de-ses-reseaux-mobiles-en-europe-avec-larret-progressif-des-reseaux-2g-et-3g-avant-la-fin-de-la-decennie/.

65. Perez, Bonnasse, Caboche, and Ricco. Fraude : des arnaques de haut vol démasqué à paris. *FranceTV*, 2023. https://www.francetvinfo.fr/replay-jt/france-3/19-20/fraude-des-arnaques-de-haut-vol-demasque-a-paris_5666693.html.

66. Aggelos Petropoulos and Panos Voutsaras. Americans and greeks started the 2004 wiretaps together. *Ekathimerini*, 2015. https://www.ekathimerini.com/in-depth/special-report/202026/americans-and-greeks-started-the-2004-wiretaps-together/#firstPage.

67. Vodafone Portugal. Cyberattack on vodafone portugal. *Press*, 2022. https://www.vodafone.pt/en/press-releases/2022/2/cyberattack-on-vodafone-portugal.html.

68. Vassilis Prevelakis and Diomidis Spinellis. The athens affair. *IEEE Spectrum*, 2007. https://spectrum.ieee.org/telecom/security/the-athens-affair.

69. Android Open Source Project. Android 12 and android 12 release notes, 2021. https://source.android.com/docs/setup/about/android-12-release?hl=en.

70. RTP. António costa preocupado com ciberataque à vodafone. https://www.rtp.pt/noticias/economia/antonio-costa-preocupado-com-ciberataque-a-vodafone_v1383151, 2022.

71. David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. Breaking LTE on layer two. In *IEEE Symposium on Security & Privacy (SP)*. IEEE, 2019.

72. ETSI SAGE. Specification of the 3gpp confidentiality and integrity algorithms uea2 and uia2. document 2 : Snow 3g specification. *ETSI*, 2006. https://www.gsma.com/security/security-algorithms/.

73. ETSI SAGE. Specification of the 3gpp confidentiality and integrity algorithms uea2 and uia2. document 1 : Uea2 and uia2 specification. *ETSI*, 2009. https://www.gsma.com/security/security-algorithms/.

74. ETSI SAGE. Specification of the 3gpp confidentiality and integrity algorithms 128-eea3 and 128-eia3. document 2 : Zuc specification. *ETSI*, 2011. https://www.gsma.com/security/security-algorithms/.

75. ETSI SAGE. Specification of the 3gpp confidentiality and integrity algorithms 128-eea3 and 128-eia3. document 1 : 128-eea3 and 128-eia3 specification. *ETSI*, 2019. https://www.gsma.com/security/security-algorithms/.

76. ETSI/TC SMG. Recommendation gsm 02.02 - network architecture. *ETSI*, 1992. https://www.etsi.org/deliver/etsi_gts/03/0302/03.01.04_60/gsmts_0302sv030104p.pdf.
77. ETSI/TC SMG. Recommandation gsm 02.09 : Security aspects. *ETSI*, 1993. https://www.etsi.org/deliver/etsi_gts/02/0209/03.01.00_60/gsmts_0209sv030100p.pdf.
78. ETSI/TC SMG. Recommendation gsm 03.03 - numbering, addressing and identification. *ETSI*, 1993. https://www.etsi.org/deliver/etsi_gts/03/0303/03.06.00_60/gsmts_0303sv030600p.pdf.
79. Symantec. Regin : Top-tier espionage tool enables stealthy surveillance, 2014.
80. Viasat. Ka-sat network cyber attack overview. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview, 2022.