FIGI

INITIATIVE MONDIALE EN FAVEUR
DE L'INCLUSION FINANCIÈRE

GROUPE DE TRAVAIL SUR LA SÉCURITÉ, L'INFRASTRUCTURE ET LA CONFIANCE

Rapport technique sur les failles du SS7 et les mesures d'atténuation applicables aux transactions des services financiers numériques

RAPPORT SUR L'AXE DE TRAVAIL «SÉCURITÉ»

Groupe de travail sur la sécurité, l'infrastructure et la confiance

Rapport technique sur les failles du SS7 et les mesures d'atténuation applicables aux transactions des services financiers numériques

05/2019

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (TIC). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

Un nouveau programme mondial visant à faire progresser la recherche sur la finance numérique et à accélérer l'inclusion financière numérique dans les pays en développement, l'Initiative mondiale en faveur de l'inclusion financière (FIGI), a été lancé par le Groupe de la Banque mondiale, l'UIT et le Comité sur les paiements et les infrastructures de marché (CPMI), avec l'appui de la Bill and Melinda Gates Foundation.

Le Groupe de travail sur la sécurité, l'infrastructure et la confiance est l'un des trois groupes de travail qui ont été créés dans le cadre de la FIGI et qui sont dirigés par l'UIT. Les deux autres sont le Groupe de travail sur l'identité numérique et le Groupe de travail sur l'acceptation des paiements électroniques. Ils sont dirigés par le Groupe de la Banque mondiale.

À propos du présent rapport

Ce rapport a été rédigé par Assaf Klinger, avec la contribution et l'aide précieuse du Dr Leon Perlman. Il a également bénéficié des remarques formulées par les membres du Groupe de travail sur la sécurité, l'infrastructure et la confiance. Vijay Mauree, de l'UIT, a assuré la supervision générale de ce rapport.

Pour toute question relative au présent rapport, veuillez contacter Vijay Mauree à l'UIT (courrier électronique: tsbfigisit@itu.int).

Table des matières

Sommaire de direction

Pour permettre aux utilisateurs d'envoyer et de recevoir de l'argent, les services financiers numériques (DFS) s'appuient largement sur les infrastructures sous-jacentes de télécommunications. Dans la plupart des pays en développement, où les DFS sont particulièrement populaires, les utilisateurs finaux disposent rarement d'une connexion fiable et accessible à Internet, ce qui accroît significativement leur dépendance à l'égard des infrastructures de communication mobile. Les données de service complémentaire non structurées (USSD) et le service de messages courts (SMS) sont les principaux canaux utilisés par les utilisateurs finaux pour communiquer avec les fournisseurs de DFS. Les canaux USSD et SMS sont depuis longtemps considérés comme compromis et de nombreuses vulnérabilités ont été découvertes. Certaines d'entre elles ont plus de 20 ans et les utilisateurs sont donc exposés à des fraudes et au vol de leur argent.

Dans leur volonté de limiter ces risques, les organismes de réglementation des télécommunications et des services financiers se heurtent principalement à un problème d'alignement des intérêts et de répartition des responsabilités. Pour limiter ces vulnérabilités, l'UIT et la Global System Mobile Association (GSMA) ont rapidement publié des lignes directrices et des avis à l'intention des opérateurs de télécommunications; toutefois, le taux d'exécution des mesures proposées est resté extrêmement faible. D'après les résultats des enquêtes menées par ce groupe de travail et par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), moins de 30% des réseaux de télécommunications de l'Union européenne et moins de **0,5%** des réseaux des pays en développement ont mis en œuvre ces stratégies d'atténuation des risques. La faiblesse de ces chiffres s'explique à la fois par une sensibilisation insuffisante aux vulnérabilités existantes et par le coût prohibitif des mesures d'atténuation que doivent mettre en œuvre les opérateurs. Aucune incitation financière ne les encourage à lutter contre ces vulnérabilités, étant donné que leur responsabilité n'est pas engagée lorsqu'une fraude au DFS est constatée.

Pour faire évoluer la situation et réduire de nombreuses vulnérabilités, le Groupe de travail propose les recommandations suivantes:

- Sensibiliser les organismes de réglementation des télécommunications et des services financiers aux différentes vulnérabilités qui affectent l'écosystème de DFS accessibles depuis les outils de télécommunications;
- Les organismes de réglementation des télécommunications et des services financiers doivent promulguer une réglementation permettant de répartir les responsabilités de manière adéquate et de contraindre les opérateurs de télécommunications à mettre en place des mesures d'atténuation des risques;
- Les organismes de réglementation des télécommunications et des services financiers doivent s'assurer que les structures juridiques concernées tiennent compte des enjeux relatifs à la sécurité de la signalisation, tant au niveau de la notification des incidents que de l'adoption de normes minimales en matière de sécurité;
- Pour chaque catégorie de réseau (3G/4G/5G), les organismes de réglementation des télécommunications doivent établir des mesures de sécurité de base que les opérateurs devront ensuite mettre en œuvre afin de garantir un environnement d'interconnexion plus sûr. La commission d'études 11 de l'UIT-T pourrait proposer des lignes directrices techniques pour l'élaboration de ces mesures de sécurité de base;
- Établir un dialogue entre, d'une part, les fournisseurs de DFS et les organismes de réglementation des télécommunications et, d'autre part, le secteur de la sécurité des télécommunications. Des tables rondes pourront permettre aux uns de découvrir les solutions d'atténuation des risques existantes et encourager les autres à en élaborer de nouvelles;
- Imposer des amendes ou accorder des subventions pour inciter les opérateurs de télécommunications, les fournisseurs de DFS et le secteur de la sécurité à travailler en commun et à mettre en œuvre des solutions au service d'un écosystème plus sûr pour les DFS.

Abréviations et acronymes

CISO	Responsable de la sécurité des systèmes d'information.
DFS	Services financiers numériques
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
GTP	Protocole de tunnellisation GPRS
GSMA	Global System Mobile Association
HLR et VLR	Enregistreur de localisation nominale / enregistreur de localisation des visiteurs – la base de données centrale contenant des informations sur l'ensemble des abonnés d'un réseau de télécommunications, qu'ils soient natifs ou itinérants.
IMEI	Identité internationale de l'équipement mobile – l'identifiant utilisé par les réseaux de télécommunications pour authentifier un équipement d'utilisateur
IMSI et TMSI	identité internationale d'abonnement mobile – l'identifiant unique assigné à chaque abonné mobile et destiné à un usage interne par les réseaux de télécommunications
LTE	Évolution à long terme – la quatrième génération de réseaux mobiles, plus connue sous le nom de 4G
MAP	Sous-système application mobile – un protocole SS7 qui permet de définir l'infrastructure de signalisation nécessaire aux services mobiles (itinérance, appels, SMS, etc.)
MSISDN	Numéro d'annuaire d'abonné international de station mobile
MOU	Protocole d'accord
Nœud B évolué	Station de base des réseaux mobiles fondés sur les technologies LTE, ou "antenne-relais GSM" (élément d'accès radio LTE)
OTP	Mot de passe à usage unique
PIN	Numéro d'identification personnel
POP	Protocole postal
SMS	Service de messages courts
SMS MO	SMS d'origine mobile – un SMS envoyé depuis un terminal mobile vers le réseau
SS7	Système de signalisation n°7 – le protocole de signalisation utilisé pour l'interconnexion entre les différents réseaux de télécommunications et entre les composantes internes de chacun de ces réseaux (qu'ils soient mobiles ou terrestres)
STK	Boîte à outils SIM
UE	Équipement de l'utilisateur – l'appareil final utilisé, dans notre cas le téléphone mobile (classique ou smartphone)
USSD MO	Transaction USSD réalisée depuis un terminal mobile – une transaction USSD initiée par un utilisateur
USSD MT	Transaction USSD aboutissant à un terminal mobile – une transaction USSD initiée depuis le réseau vers un terminal mobile
USSD	Données de service complémentaire non structurées

Rapport technique sur les failles du SS7 et les mesures d'atténuation applicables aux transactions des services financiers numériques

1 INTRODUCTION

Les services financiers numériques (DFS) reposent principalement sur les réseaux de télécommunications. En effet, dans les pays où ce type de service est particulièrement populaire, les utilisateurs finaux disposent rarement d'une connexion fiable et accessible à Internet, et les DFS ont donc privilégié le canal des télécommunications. Dans les économies des pays en développement, qui représentent l'essentiel des utilisateurs finaux des DFS, l'usage de téléphones mobiles classiques reste dominant. Par conséquent, les utilisateurs finaux communiquent principalement par l'intermédiaire des données de service complémentaire non structurées (USSD), du service de messages courts (SMS) et de la boîte à outils SIM (STK). En outre, à l'heure actuelle, le réseau de signalisation n'est pas isolé, ce qui permet aux intrus d'exploiter ses failles pour intercepter des communications vocales et SMS, contourner la facturation, voler l'argent présent sur le compte d'un utilisateur mobile ou compromettre les communications du réseau mobile, y compris dans les pays développés.

Les canaux de communication USSD et SMS sont depuis longtemps considérés comme exposés aux attaques et de nombreuses vulnérabilités ont été découvertes. Dès lors, les attaquants sont en mesure d'exploiter ces vulnérabilités pour commettre des fraudes ou voler de l'argent et les victimes, peu méfiantes, ignorent bien souvent que leur compte a été compromis ou piraté.

Ce document a pour but d'examiner les différentes vulnérabilités auxquelles sont exposés les réseaux de télécommunications, ainsi que leur impact sur les services financiers numériques, tant du côté de l'utilisateur final que du côté du fournisseur de services. Il permettra aux fournisseurs de DFS de mieux appréhender les vulnérabilités existantes et de mettre au point des stratégies d'atténuation des risques en vue de protéger leurs clients.

2 LES VULNÉRABILITÉS DES TÉLÉCOMMUNICATIONS ET LEUR IMPACT SUR LES DFS

Les réseaux de télécommunications souffrent de vulnérabilités qui peuvent donner lieu à diverses attaques criminelles et entraîner des fraudes visant à voler de l'argent numérique; bien souvent, la fraude consiste, pour l'attaquant, à se faire passer pour le fournisseur de DFS auprès de l'utilisateur final, ou pour l'utilisateur final auprès du fournisseur de DFS. Dans les deux cas, l'attaquant exploite les vulnérabilités du réseau de télécommunications pour s'authentifier et réaliser des actions depuis le compte qu'il a compromis. Ces attaques peuvent notamment prendre les formes suivantes:

2.1 Fraude financière au guichet

Dans cet exemple, le fraudeur se présente à un agent de DFS (par exemple, au guichet d'une agence 7-eleven) et demande à procéder à un retrait en espèces sur son compte. Il donne le numéro de compte de la victime à l'agent et ce dernier lance la transaction en envoyant un code de vérification par SMS. Le fraudeur intercepte le SMS et l'utilise pour finaliser l'opération et voler l'argent de sa victime.

2.2 Usurpation de compte

Dans cet exemple, le fraudeur utilise la technologie USSD pour usurper un compte qui ne lui appartient pas. Pour réussir son attaque, il doit d'abord usurper le numéro de téléphone de sa victime et composer le code USSD (pour cela, il peut procéder à une interception "over-the-air", expliquée plus en détail dans la section 7). Après avoir utilisé le numéro de téléphone de la victime pour ouvrir une session USSD auprès du fournisseur de DFS, le fraudeur peut changer son code PIN et ajouter un nouveau numéro de téléphone à ses informations de compte. Il peut ensuite utiliser le numéro de téléphone qu'il vient d'ajouter pour ouvrir une nouvelle session USSD et utiliser le nouveau code PIN pour se connecter au compte et transférer l'argent.

2.3 Ingénierie sociale

L'ingénierie sociale peut prendre des formes diverses; dans notre exemple, le fraudeur utilise la technologie USSD pour induire la victime en erreur et l'inciter à communiquer son numéro de compte et son code PIN. Pour mener à bien cette attaque, il se fait passer pour le fournisseur de DFS et envoie un message USSD à la victime pour lui indiquer qu'un transfert d'argent est en attente et qu'elle doit composer son numéro de compte et son code PIN dans la boîte de dialogue USSD afin de recevoir les fonds sur son compte. Ces informations permettent à l'attaquant d'usurper le compte de la victime.

3 VULNÉRABILITÉS DES TÉLÉCOMMUNICATIONS ET SURFACES D'ATTAQUE

Les vulnérabilités dont souffrent les réseaux de télécommunications se répartissent en deux surfaces d'attaque: le réseau SS7 et l'interface radio cellulaire:

- Le réseau SS7 est un réseau de signalisation hérité utilisé pour l'interconnexion de **l'ensemble des opérateurs de réseau mobile à travers le monde**. Le protocole SS7[1] utilisé pour la signalisation existe depuis les années 1980 et la migration récente vers le protocole Diameter[2] (pour les réseaux 4G-LTE) n'a apporté aucune solution aux vulnérabilités fondamentales du protocole SS7.
- Depuis le début des communications cellulaires, l'interface radio cellulaire (la communication par radiofréquence établie entre le téléphone mobile et le réseau mobile) constitue une surface d'attaque particulièrement importante. L'interception de ces communications radio favorise la collecte de renseignements et l'espionnage, et ne nécessitent pas d'accès au réseau mobile. Malgré l'adoption des dernières générations de réseaux mobiles (3G/4G), plus robustes en matière de sécurité, la plupart des dispositifs d'interception directe ont réussi à contourner les mesures d'atténuation des risques mises en place. En outre, malgré la forte vulnérabilité de leur interface radio de chiffrement et les logiciels à code source ouvert qui permettent de les compromettre, de nombreux réseaux 2G sont restés actifs.

4 LES PRINCIPAUX TYPES D'ATTAQUES DANS LE DOMAINE DES TÉLÉCOMMUNICATIONS

Tableau 1 – Les principaux types d'attaques dans le domaine des télécommunications

Attaque	Description	Impact sur les DFS
Spam	Acheminer un message court vers l'appareil mobile de destination a un coût, qui est facturé à l'émetteur. Un attaquant peut procéder à un envoi groupé qui permettra à ses SMS de contourner leur itinéraire normal et d'échapper à la facturation. Il est également possible d'usurper divers paramètres d'envoi de SMS, tels que l'identité de l'émetteur, ou d'échapper aux systèmes de contrôle pour envoyer directement des SMS à ses victimes.	Appels ou envois groupés de SMS destinés à voler des données personnelles ou à obtenir des avantages financiers en utilisant des numéros payants.
Usurpation	Les informations d'identification (adresses, noms et numéros de sous-systèmes) utilisées aux différents niveaux des protocoles SS7 et Diameter ne sont pas authentifiées et peuvent être usurpées par un tiers malveillant.	Fraude à la facturation, lorsque l'opérateur de télécommunications est également le fournisseur de DFS et que la monnaie utilisée est en crédits (système de recharge, sans utilisation d'argent électronique). L'attaquant peut recharger une carte SIM en usurpant l'identité d'un autre abonné et ainsi échapper à la facturation.
Traçage de la localisation	L'attaquant peut localiser un abonné cible en se basant sur son MSISDN. Les opérateurs de réseaux mobiles ont le devoir d'acheminer efficacement les messages vers leurs abonnés. Par conséquent, le réseau domestique est toujours en mesure de contacter tous les abonnés, où qu'ils se trouvent. Dans certains cas, l'attaquant n'a même pas besoin d'envoyer des messages, car l'écoute clandestine passive suffit à révéler l'emplacement de sa cible. Obtenir la localisation de l'abonné constitue également un préalable indispensable à d'autres attaques telles que l'interception.	Obtenir la localisation approximative d'une victime donnée. Cette information est ensuite utilisée à des fins d'ingénierie sociale, pour inciter l'utilisateur à divulguer les identifiants de son compte de DFS.
Fraude aux abonnés	L'attaquant peut modifier le profil de l'abonné ou envoyer des messages de signalisation afin de déclencher une facturation fallacieuse et d'obtenir un service sans avoir à le payer.	Ce type d'attaque peut viser à: Obtenir ou voler des crédits prépayés destinés à passer des appels vocaux, envoyer des SMS ou consommer des données mobiles, et les convertir en argent mobile, en biens ou en services; Compromettre les opérations de facturation, par exemple en imposant des surcoûts à un autre abonné ou en faisant en sorte d'échapper au paiement (pour les DFS dont le fournisseur est aussi l'opérateur du réseau de télécommunications); Exploiter les failles des services financiers mobiles en s'appuyant sur la technologie USSD et le protocole MAP.

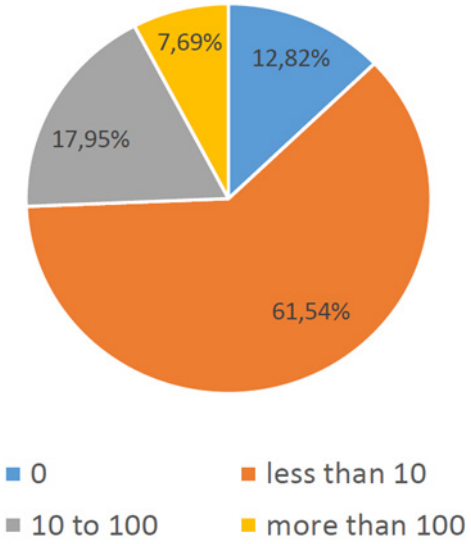
(continue)

Attaque	Description	Impact sur les DFS
Interception	L'attaquant peut modifier la localisation et le profil de l'abonné de façon à recevoir les appels, les SMS et le trafic de données entrants et/ou sortants. Cette attaque permet d'espionner les communications de la victime et peut prendre la forme d'une stratégie d'interception destinée à altérer la communication. L'accès à l'interface de signalisation permet à l'attaquant de mener des opérations d'interception locale efficaces, fondées sur des antennes factices.	Lorsqu'une authentification à deux facteurs (A2F) est requise, les SMS sont généralement utilisés en second facteur. Dans le cadre d'une attaque de plus grande ampleur, l'attaquant peut également espionner les SMS pour contourner l'A2F. Interception des communications
Déni de service	L'attaquant peut provoquer un déni de service affectant l'ensemble du réseau, un petit groupe d'abonnés ou même un seul abonné cible. La mobilité s'accompagne d'une fonctionnalité permettant de supprimer un abonné d'une zone géographique donnée. L'attaquant pourra exploiter cette fonctionnalité pour imposer un déni de service à un utilisateur spécifique.	Parmi les impacts de grande ampleur les plus courants, on peut notamment citer la réinitialisation de l'équipement réseau régional, qui entraînerait la suppression des contextes utilisateur de l'ensemble des abonnés concernés. Cette attaque peut être répliquée à volonté et entraîner une indisponibilité persistante du service.
Infiltrations	L'attaquant peut compromettre l'interconnexion pour obtenir un accès à des systèmes auxquels il ne pourrait pas accéder en temps normal. Lorsqu'elles traversent le réseau central mobile, les données de l'utilisateur sont tunnelisées. Un défaut de configuration peut permettre à l'attaquant d'obtenir un accès illégal à une partie du réseau central mobile. L'attaquant peut également pénétrer les systèmes du réseau central par l'intermédiaire des données mobiles ou des interfaces opérationnelles, ce qui est susceptible d'entraîner de nouvelles attaques.	Accès non autorisé à des éléments du réseau central mobile. Parmi les impacts les plus courants, on peut notamment citer le vol de données personnelles ou l'accès à d'autres éléments sensibles tels que des réseaux de données par paquets.
Attaques au niveau du routage	Les interconnexions entre réseaux fondées sur l'envoi de paquets s'appuient sur le routage (un processus de sélection des chemins pour le trafic d'un réseau donné) et sont donc exposées à des attaques par détournement du routage.	Lorsque les données ne sont pas chiffrées ou que leur intégrité ne fait pas l'objet de vérifications, cela permet aux attaquants d'espionner ou de modifier le trafic d'interconnexion.

5 PROFIL DES ATTAQUES MENÉES CONTRE LES RÉSEAUX DE TÉLÉCOMMUNICATIONS

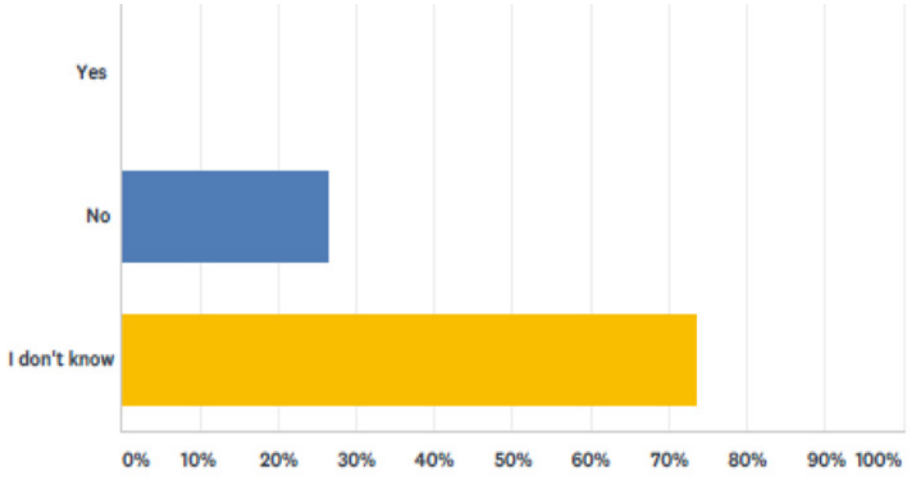
Une enquête menée par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[3] a permis d'interroger 39 fournisseurs de services de communication électronique à travers l'Union européenne pour étudier le profil et la fréquence des attaques contre les réseaux de télécommunications. Plus de 80% des opérateurs de télécommunications interrogés ont indiqué avoir détecté ou essuyé plusieurs attaques, et environ 25% d'entre eux ont indiqué avoir fait face à un nombre important d'attaques, comme le montre le diagramme ci-dessous. Toutefois, comme le montre la figure 2, les mécanismes de détection des attaques mis en place par les opérateurs de télécommunications sont encore insuffisants, ce qui explique le faible nombre de signalements.

Figure 1 – Fréquence des attaques menées contre les réseaux de télécommunications dans l'Union européenne (enquête)



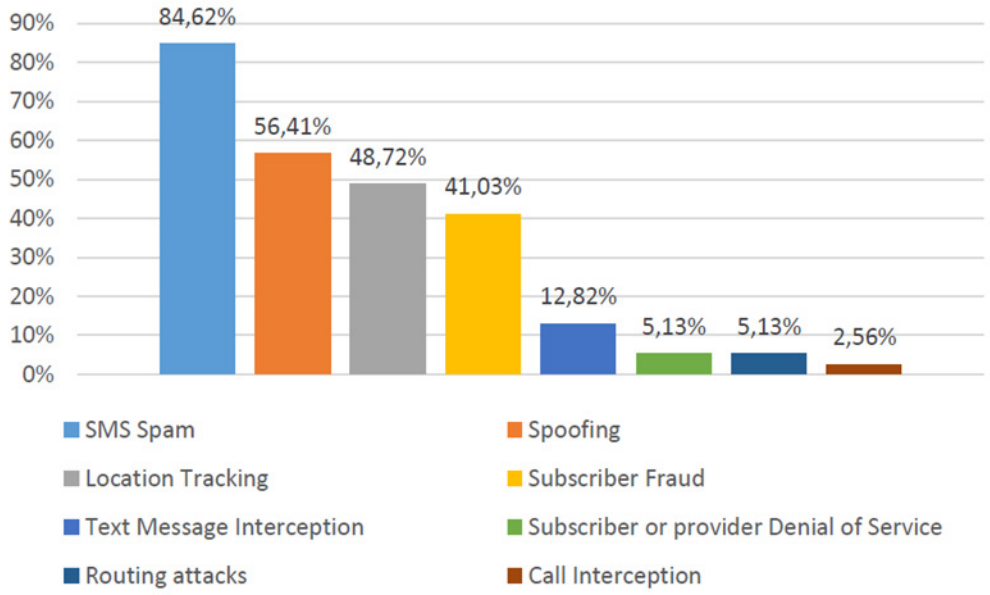
D'après l'enquête menée par le Groupe de travail sur la sécurité, l'infrastructure et la confiance, plus de 70% des organismes de réglementation et des opérateurs de télécommunications interrogés ignoraient si leur réseau faisait l'objet d'attaques au moment de l'enquête.

Figure 2 – Niveau de sensibilisation aux attaques contre les réseaux de télécommunications dans les pays en développement (enquête)



Les opérateurs de télécommunications qui ont détecté des attaques ont classées celles-ci dans les catégories ci-dessous. Le diagramme fait apparaître une nette prépondérance des attaques directement liées à des fraudes aux DFS, telles que l'usurpation, l'interception de SMS et la fraude aux abonnés.

Figure 3 – Types d'attaques contre les réseaux de télécommunications dans l'Union européenne (enquête)



6 LE DÉFI À RELEVER

On considère que la protection de ces deux surfaces d'attaque relève de la responsabilité exclusive de l'opérateur du réseau mobile – si l'opérateur met en œuvre des mesures pour protéger son réseau, l'ensemble des utilisateurs de ce réseau seront également protégés. Toutefois:

- La plupart des opérateurs de réseau mobile n'ont pas encore protégé leur réseau contre ce type d'attaque, bien que la Global System Mobile Association (GSMA) et l'UIT (organismes mondiaux de gouvernance des télécommunications) aient publié des lignes directrices[4] pour les aider à mettre au point une stratégie de défense.
- Le plus souvent, les opérateurs qui ont appliqué ces recommandations[5] se sont contentés d'une mise en œuvre partielle, qui n'a permis de résoudre qu'une partie des vulnérabilités dont souffraient leur réseau.
- Les opérateurs des réseaux de télécommunications ne sont pas en mesure de se protéger contre la plupart des vulnérabilités de l'interface radio, d'autant plus lorsque leurs abonnés ont recours à l'itinérance.

La difficulté reste donc entière: comment les fournisseurs de DFS ou les clients peuvent-ils se défendre contre les attaques cellulaires, sans attendre que les opérateurs de réseau mobile règlent le problème à leur place?

7 IDÉE REÇUE: ATTAQUER LES RÉSEAUX DE TÉLÉCOMMUNICATIONS N'EST PAS À LA PORTÉE DE TOUS, SEULS LES GOUVERNEMENTS DISPOSENT DE MOYENS SUFFISANTS

Cette idée est largement répandue parmi les responsables de la sécurité des systèmes d'information (CISO) et les responsables de la cybersécurité des entreprises. Les barrières à l'entrée se sont considérablement abaissées et n'importe quel pirate informatique peut désormais exploiter les vulnérabilités des réseaux mobiles avec un budget d'environ 500 dollars des États-Unis.

Par exemple:

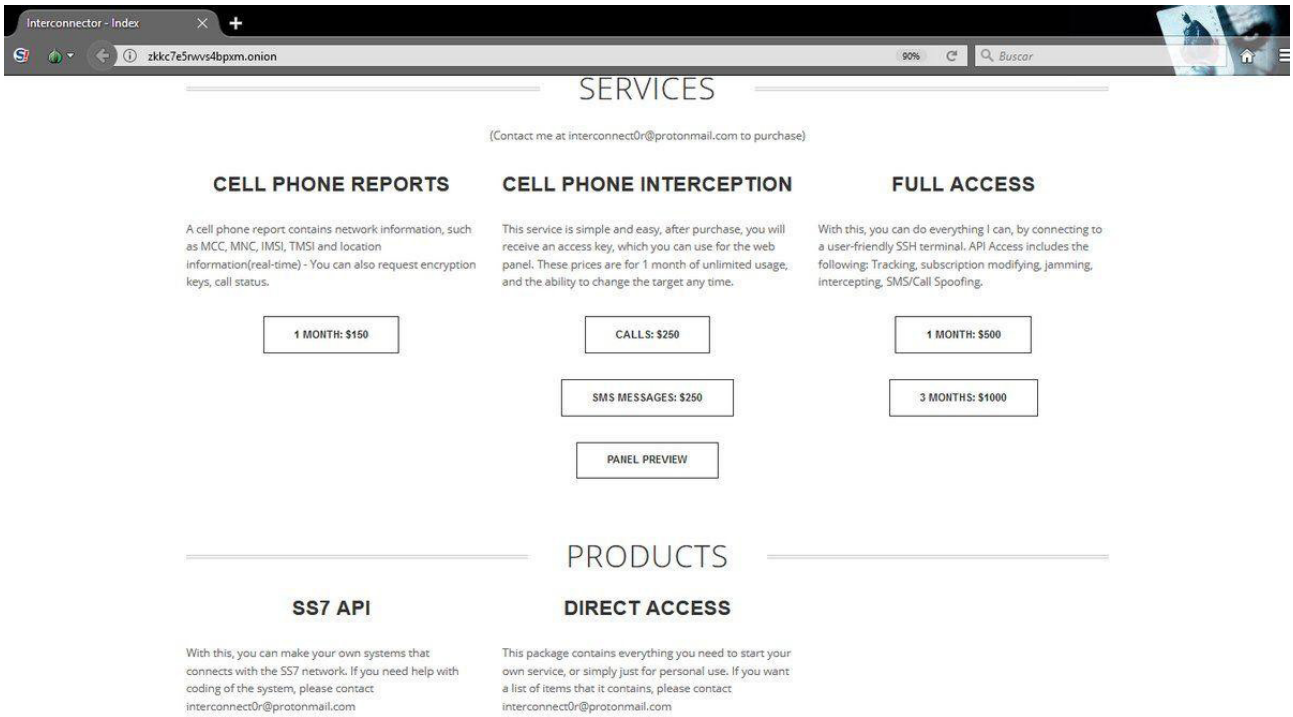
En s'appuyant sur un système amateur d'attaque par interception, il est possible d'intercepter les communications cellulaires à proximité. Une fois la

méthode de chiffrement compromise[6], l'ensemble des appels, des SMS et du trafic HTTP entrants ou sortants de l'appareil intercepté peuvent être déchiffrés. À l'heure actuelle, un système d'attaque par interception rudimentaire comme celui de la figure 4 ne nécessite rien de plus qu'un logiciel à code source ouvert disponible sur Internet et environ 600 dollars de matériel acheté sur eBay.

Figure 4 – Un système d'interception MITM rudimentaire fondé sur du matériel disponible dans le commerce et un logiciel à code source ouvert

Pour démontrer la relative simplicité des attaques cellulaires, il est également possible de prendre l'exemple de l'accès au réseau SS7. Autrefois, le réseau SS7 était considéré comme un environnement protégé, auquel seuls les opérateurs de réseau mobile détenteurs d'une licence pouvaient accéder. Avec le développement des envois groupés de SMS, de l'Internet des objets et des services géolocalisés, d'autres entités dépourvues de licence ont désormais accès à ce réseau.

Figure 5 – Des accès SS7 proposés à la vente sur un site du dark Web



De ce fait, de plus en plus d'intermédiaires et d'entreprises ou d'individus bénéficiant d'un accès direct au réseau vendent leur accès sur le dark Web. Pour 150 à 2 500 dollars, un pirate peut accéder au réseau SS7 et exploiter ses vulnérabilités cellulaires, sans s'appuyer sur une quelconque infrastructure.

8 LA CHAÎNE DE FRAPPE DES ATTAQUES CELLULAIRES

Pour accéder à des données sensibles telles que les identifiants de compte bancaire et mener à bien des attaques telles que l'usurpation de compte en ligne, les attaquants ont besoin de certaines informations cruciales. Le tableau 2 ci-dessous présente la façon dont les attaquants peuvent exploiter les différentes surfaces d'attaque cellulaires de façon à obtenir les informations dont ils ont besoin pour réaliser les différentes étapes de la chaîne de frappe.

Tableau 2 – La chaîne de frappe des attaques contre les réseaux de télécommunications

Étape	Surface d'attaque du réseau de télécommunications	Surface d'attaque SS7	Surface d'attaque MITM
Collecte d'informations	Numéro de téléphone de la victime	Ingénierie sociale	Ingénierie sociale
	Numéro IMSI de la victime	Requête SS7 (l'attaquant doit d'abord obtenir le numéro TMSI)	Interception des numéros IMSI (de tous les téléphones à proximité)
Fuite de la localisation	Traçage de la localisation de la victime	Requête SS7	Triangulation
Fuite de données	Interception de communications vocales et SMS	Simuler l'itinérance de la victime (en utilisant la procédure UL[7]) afin d'intercepter des SMS entrants Rerouter les appels reçus par la victime en utilisant le renvoi d'appel afin d'intercepter les appels entrants Modifier le profil de la victime sur l'enregistreur de localisation nominale (HLR) ou l'enregistreur de localisation des visiteurs (VLR) afin d'intercepter les appels et les SMS sortants (par l'intermédiaire du mécanisme de facturation)	Rétrograder la liaison de radiofréquence cellulaire vers la 2G ou la 3G et obtenir les clés de chiffrement (plusieurs méthodes possibles), ce qui permettra d'intercepter à la fois les appels et les SMS entrants et sortants
	Intercepter les transactions USSD – obtenir les identifiants de connexion mobile au compte bancaire	Obtenir les identifiants de connexion mobile au compte bancaire en s'appuyant sur la fraude psychologique – pour plus de détails, voir la figure 6	Intercepter les identifiants de la victime en s'appuyant sur une transaction USSD qu'elle a déjà réalisée
	Intercepter le canal de données mobiles et procéder à une attaque MITM	Rerouter le tunnel GTP de l'abonné de façon à utiliser le protocole postal de l'attaquant pour établir la connexion à Internet	Appliquer la norme relative au service de transmission de données en mode paquet (GPRS)/ aux débits binaires améliorés pour les GSM de demain (EDGE)/au système de télécommunications mobiles universelles (UMTS) à l'appareil mobile et tunneliser la connexion par données mobiles à travers le système
Cyberattaque	Identifiants de comptes en ligne (banque, courrier électronique, etc.)	Utiliser l'extraction des identifiants USSD pour se connecter au compte du service financier mobile Utiliser l'interception du mot de passe à usage unique envoyé par SMS pour se connecter au compte en ligne	
	Implantation d'un logiciel malveillant sur l'appareil mobile	Implanter un logiciel malveillant sur le téléphone en exploitant une vulnérabilité du navigateur (sur la page demandée par l'utilisateur, insérer une balise iFrame contenant un lien vers un site Internet infecté)	

9 EXEMPLES D'ATTAQUES VISANT LES INFRASTRUCTURES DE DFS

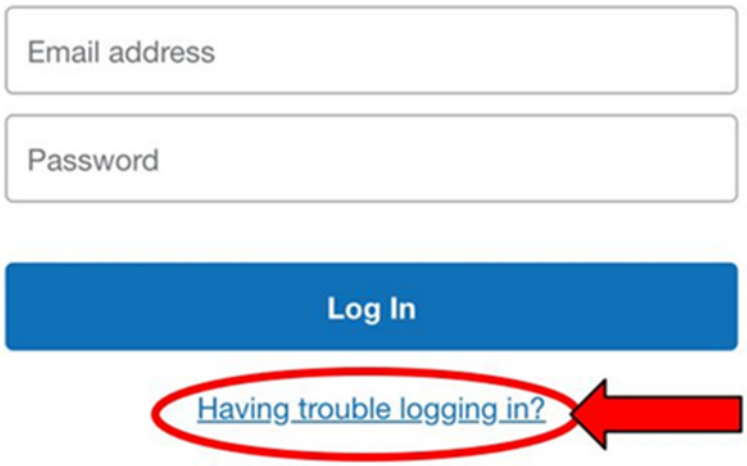
9.1 Interception d'un SMS contenant un mot de passe à usage unique

À l'heure actuelle, la méthode la plus populaire pour renforcer les processus d'authentification est l'envoi d'un mot de passe à usage unique par SMS. Partout dans le monde, la très grande majorité des fournisseurs de DFS y ont recours. Le SMS envoyé peut être intercepté en s'appuyant sur le protocole SS7 ou sur une attaque MITM "over-the-air", et le mot de passe à usage unique ainsi obtenu peut être exploité à des fins malveillantes pour accéder illégalement aux comptes des utilisateurs concernés. L'attaquant peut utiliser le mot de passe à usage unique qu'il a intercepté pour récupérer les mots de passe ou les codes PIN des comptes correspondants. Il peut également le combiner avec une attaque USSD (voir plus bas) pour modifier le numéro de téléphone associé à un compte. Voici un exemple d'interception d'un mot de passe à usage unique utilisé pour accéder illégalement à un compte en ligne:

a) Étape 1: "J'ai oublié mon mot de passe"

L'attaquant accède au portail de connexion et lance la procédure de récupération du mot de passe

Figure 6 – Lancer la procédure de récupération du mot de passe



b) Étape 2: Sélectionner l'envoi d'un mot de passe à usage unique par SMS parmi les différentes options d'authentification

L'attaquant active l'interception en s'appuyant sur le protocole SS7 ou sur une attaque MITM "over-the-air" et sélectionne l'option de récupération du mot de passe "Recevoir un mot de passe à usage unique par SMS":

c) Étape 3: Utiliser le mot de passe à usage unique présent dans le SMS intercepté et accéder au compte

Lors de cette étape, l'attaquant utilise le code qui lui a été envoyé par SMS. La victime n'a pas reçu ce SMS et ne sait donc pas qu'elle en train de subir une attaque. Après vérification du code, le système en ligne du fournisseur de DFS autorise la connexion de l'attaquant, qui peut alors transférer les fonds de la victime depuis son compte.

9.2 Recours à l'ingénierie sociale et à la technologie USSD pour obtenir des données d'identification sensibles

La technologie USSD est utilisée par les services bancaires en ligne et d'autres applications de services financiers sensibles. Les messages USSD bénéficient d'un haut degré de confiance parmi les utilisateurs. L'attaque la plus facile à exécuter et à reproduire consiste donc à utiliser la technologie USSD pour envoyer un message frauduleux à l'utilisateur en usurpant l'identité du fournisseur de services financiers et en incitant l'utilisateur à divulguer des informations sensibles telles que son numéro de compte et son code PIN. Pour obtenir ces informations d'identification, l'attaquant peut par exemple envoyer un message USSD d'hameçonnage, tel que celui présenté dans la figure 8 ci-dessous:

Étant donné que le message USSD ne contient aucune identification et que l'utilisateur est habi-

Figure 7 – Sélectionner l'envoi d'un mot de passe à usage unique par SMS parmi les différentes options d'authentification

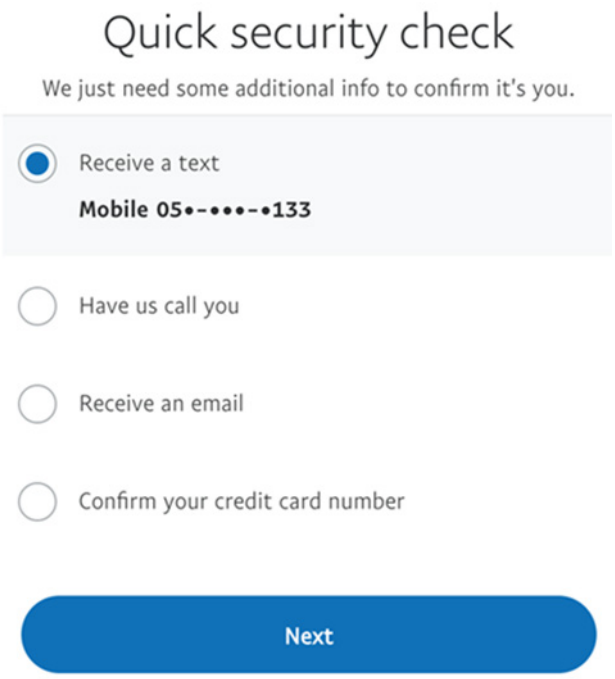
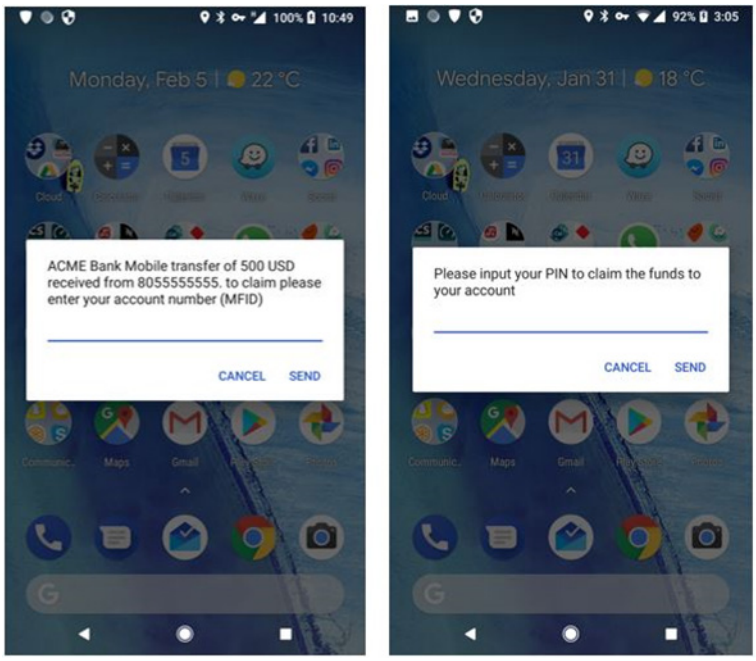


Figure 8 – Utiliser la technologie USSD à des fins d'ingénierie sociale



tué à recevoir ces messages du réseau, l'utilisateur divulgue son numéro de compte et son code PIN en toute confiance. L'attaquant se connecte ensuite au compte et intercepte les fonds.

9.3 Attaques par déni de service

En s'appuyant sur le protocole SS7, l'attaquant peut entraîner un déni de service pour une sélection d'abonnés cibles ou provoquer une panne de réseau

plus étendue. Les attaques par déni de service peuvent prendre des formes diverses, telles que: l'envoi d'un message de procédure UL conduisant vers une adresse hors-réseau, qui empêchera l'ensemble des appels et des SMS entrants d'atteindre l'abonné; la suppression d'un utilisateur donné du registre VLR[8], qui entraînera un déni de service pour cet utilisateur, jusqu'à sa réinsertion dans le registre. Lorsqu'elles sont menées à grande échelle (par exemple, de manière automatique pour un ensemble de numéros IMSI), chaque attaque peut entraîner une panne réseau de grande ampleur. Néanmoins, la plupart du temps, ces attaques SS7 par déni de service n'affectent pas le réseau radio et leurs effets s'annulent donc presque immédiatement lorsqu'une transaction sortante (émission d'un appel ou envoi d'un SMS) est réalisée.

9.4 Échange de carte SIM

L'usurpation d'un compte peut également s'effectuer par un échange de carte SIM. L'attaquant peut par exemple avoir recours à l'ingénierie sociale en se faisant passer pour la victime auprès de l'opérateur mobile et en déclarant la perte d'une carte SIM afin d'en obtenir une nouvelle. En cas de réussite, l'attaquant obtient ainsi le clonage de la carte SIM. Grâce à cette carte clonée, il peut accéder au menu USSD du fournisseur de DFS et réinitialiser le code PIN associé au compte de la victime. Pour cela, l'attaquant utilise la carte clonée pour recevoir un mot de passe à usage unique par SMS et confirmer le nouveau code PIN. Il est désormais en possession du compte et peut se connecter et transférer les fonds.
Par exemple: des escrocs ont vidé le compte d'un utilisateur d'Airtel Money[9]. Ils l'ont appelé en prétendant vouloir l'assister dans l'enregistrement de sa carte SIM et le processus de mise à niveau vers la technologie 4G. Au cours de la conversation, ils lui ont demandé de composer les caractères *102#, qui correspondaient en réalité au code permettant l'échange de carte SIM. La victime s'est alors aperçue qu'elle ne pouvait plus recevoir ni émettre d'appels et que son compte Airtel Money avait été vidé.

9.5 Recyclage de carte SIM

Le recyclage de carte SIM ne fait pas partie des attaques SS7. Il s'agit plutôt d'un manque d'attention et de diligence de la part du fournisseur de DFS, qui permet à une personne non autorisée d'accéder à des fonds qui ne lui appartiennent pas.
Les étapes du recyclage de carte SIM sont les suivantes:

- Une personne A reçoit une carte SIM prépayée et utilise le numéro de téléphone associé pour ouvrir un compte de DFS.
- Après quelques mois d'utilisation, la personne A cesse de recharger la carte SIM prépayée, mais le compte de DFS associé à ce numéro de téléphone affiche toujours un solde positif.
- Après une période d'inactivité (généralement 1 à 6 mois), sans utilisation ni rechargement de la carte SIM, l'opérateur de réseau mobile annule la carte, ce qui entraîne la déconnexion de la personne A et de son compte de DFS (dont le solde est peut-être positif).
- L'opérateur de réseau envoie à une personne B une nouvelle carte SIM prépayée porteuse de l'ancien numéro de téléphone de la personne A (le recyclage est entériné).
- La personne B peut désormais accéder au compte de DFS de la personne A et disposer des fonds restants.

10 STRATÉGIES D'ATTÉNUATION DES RISQUES À DESTINATION DES OPÉRATEURS DE RÉSEAU MOBILE

La surface d'attaque SS7 relève de la compétence de l'opérateur de réseau mobile. De grandes organisation internationales de télécommunications telles que l'UIT et la GSMA ont constaté le problème et publié des lignes directrices pour permettre aux opérateurs de prévenir ce type d'attaque. Ces directives sont présentes dans plusieurs documents. Le sous-groupe de travail de la GSMA consacré à la fraude et à la sécurité en matière d'itinérance et d'interconnexion (RIFS) a publié une série de documents sur le thème de la sécurité de la signalisation fondée sur les protocoles SS7 et Diameter, en réaction aux attaques décrites plus haut. Ces documents abordent les différents aspects de la sécurité de la signalisation. Il s'agit de documents internes, accessibles uniquement aux membres de la GSMA. Par conséquent, il n'existe pas de référence exacte permettant d'y accéder. Les entreprises qui bénéficient d'un accès à l'outil interne de la GSMA pourront les consulter facilement en s'appuyant sur les infor-

mations ci-dessous. Nous donnerons un aperçu des normes en vigueur dans le secteur et décrirons de manière générale les mesures concrètes d'atténuation qui peuvent en découler.
Les membres de la GSMA peuvent consulter ces documents à partir du lien suivant (en anglais): https://www.gsma.com/newsroom/gsmadocuments/technical-documents/

10.1 FS.11: Lignes directrices relatives au contrôle de la sécurité des interconnexions SS7
Ce document décrit les modalités de contrôle du trafic SS7 à des fins de détection des attaques. Pour améliorer la sécurité de la signalisation, la première étape consiste à évaluer l'état du réseau. Pour cela, il importe avant tout de déterminer si le réseau est la cible d'attaques et, le cas échéant, quelle est leur intensité et leur nature. Ce document propose aux opérateurs de réseau mobile des stratégies relatives au contrôle du trafic, à son efficacité, à sa durée et à la classification des messages MAP entrants sur l'interface d'interconnexion. Il dresse une liste de stratégies d'atténuation des risques portant sur un grand nombre d'attaques SS7 menées contre les réseaux 2G et 3G. Les règles de filtrage présentées dans ce document permettent aux opérateurs de déterminer si un message qui pénètre l'interface d'interconnexion est légitime, interdit, non autorisé, suspect ou inhabituel.

10.2 FS.07 Sécurité des réseaux SS7 et SIGTRAN
Ce document offre une réflexion de fond sur la gestion des messages SS7 en périphérie de réseau. Il décrit la pile de protocole SS7 dans son ensemble et insiste particulièrement sur le protocole MAP, qui correspond au niveau où les attaques sont les plus fréquentes. Le document propose une analyse de sécurité des protocoles SS7 et SIGTRAN. Il dresse une liste de mesures visant à lutter contre un grand nombre d'attaques SS7 et formule des recommandations relatives au déploiement de ces mesures. Le document FS. 07 contient également des précisions sur la façon dont les pare-feux SS7 et les nœuds d'extrémité doivent être configurés pour empêcher les messages non autorisés et les attaques d'atteindre le réseau central. La configuration proposée est adaptée à l'ensemble des messages MAP v2/3. Enfin, le document présente des mesures visant à lutter contre les attaques SS7 connues à ce jour.

10.3 IR.82 Lignes directrices pour la mise en œuvre de la sécurité dans le SS7
Ce document présente des mesures générales de sécurité SS7, notamment des mesures relatives aux SMS et un grand nombre de mesures liées à la pile de protocole SS7. Chacune des mesures proposées n'est pas adaptée à n'importe quel réseau et le document dans son ensemble doit donc être considéré comme une boîte à outils à destination des opérateurs.

10.4 IR.88 Lignes directrices relatives à l'itinérance pour la norme LTE et l'EPC
Ce document présente les mesures de sécurité relatives à l'interconnexion (itinérance) pour la norme LTE. Il s'agit de l'équivalent du document IR.82 pour la norme LTE. Il contient une boîte à outils destinée à améliorer la sécurité du protocole Diameter. Cette boîte à outils couvre des aspects tels que les attaques au niveau du routage, le déni de service, le suivi de la localisation et d'autres types d'attaques contre les interconnexions fondées sur Diameter et dirigées contre les protocoles de transmission de commande de flux (SCTP) et de tunnellisation GPR (GTP). Le document propose également des recommandations adaptées aux différentes interfaces (S6a, S9, S8, etc.). Enfin, il aborde la question de l'interfonctionnement avec les systèmes hérités, la sécurité des SMS et les enjeux liés à la facturation et aux réglementations.

10.5 Les mesures d'atténuation proposées par les documents de la GSMA et leur efficacité face aux principaux types d'attaques menées contre les télécommunications

Tableau 3 – Les stratégies d'atténuation des risques proposées par les documents de la GSMA et leur couverture face aux principaux types d'attaques contre les protocoles SS7 ou Diameter

Attaque	FS.11 (2/3G)	FS.07 (2/3G)	IR.82 (2/3G)	IR.88 (4G)
Spam	x	√	√	x
Usurpation	√	√	√	x
Traçage de la localisation	√	√	√	√
Fraude aux abonnés	x	√	√	√
Interception	x	√	x	x
Déni de service	√	√	√	x
Infiltrations	√	√	√	√
Attaques au niveau du routage	x	√	√	x

11 LA MISE EN ŒUVRE DES MESURES D'ATTÉNUATION DES RISQUES PAR LES OPÉRATEURS DE RÉSEAU MOBILE

Les opérateurs de réseau mobile n'ont pas encore véritablement résolu le problème des vulnérabilités auxquelles sont exposés les réseaux SS7 de télécommunications. Ce constat repose sur les résultats de deux enquêtes: celle de l'ENISA dans l'Union européenne et celle du Groupe de travail sur la sécurité, l'infrastructure et la confiance dirigé par l'UIT dans les pays en développement. D'après l'enquête de l'ENISA, en réaction à ces vulnérabilités, la plupart des opérateurs de télécommunications se sont contentés de mettre en œuvre le routage domestique des SMS[10] et de pratiquer un filtrage[11] au niveau des nœuds de signalisation. La mise en œuvre de l'une ou l'autre des stratégies d'atténuation des risques évoquées dans la section 11 ne concerne qu'environ un quart des opérateurs. Dans les pays en développement, la majorité des organismes de réglementation et des opérateurs de télécommunications interrogés n'étaient pas au courant de l'existence de ces stratégies et, lorsqu'ils étaient au courant, leur taux d'exécution restait particulièrement faible (moins de 10%).

Ce faible taux d'exécution s'explique par une raison très simple: la mise en œuvre de stratégies d'atténuation des risques solides représente un coût important pour l'opérateur de télécommunications. Au sein de l'Union européenne, environ 75% des opérateurs interrogés ont répondu que le principal frein à la mise en œuvre de ces mesures était leur coût, ainsi que l'absence d'une réglementation contraignante.

12 STRATÉGIES D'ATTÉNUATION DES RISQUES À DESTINATION DES FOURNISSEURS DE DFS

Du côté des fournisseurs de DFS, la première chose à faire pour éviter ces attaques consiste à déployer un système d'authentification alternatif hors bande, extérieur à l'écosystème de télécommunications. Cela peut fonctionner pour les clients qui utilisent un smartphone et se servent d'une application pour accéder au DFS. Les fournisseurs de DFS doivent

Figure 9 – Le taux d'exécution des mesures d'atténuation des risques chez les opérateurs de réseau mobile de l'Union européenne

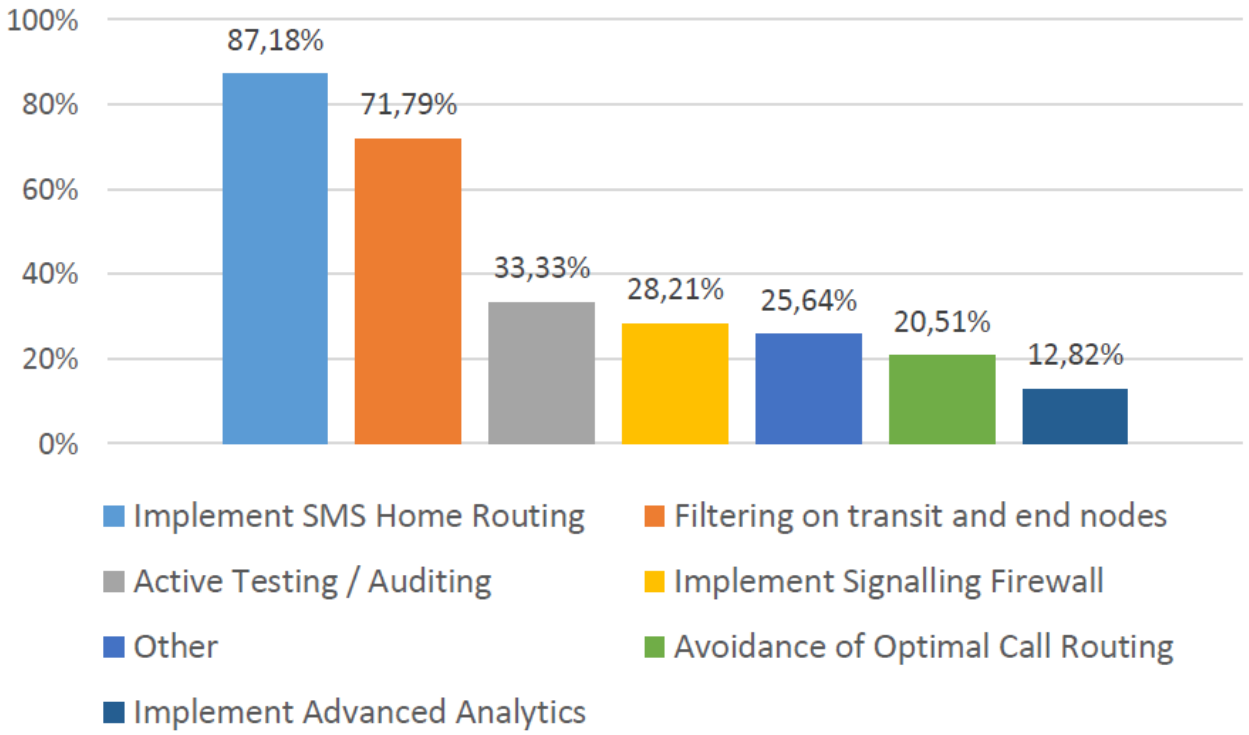
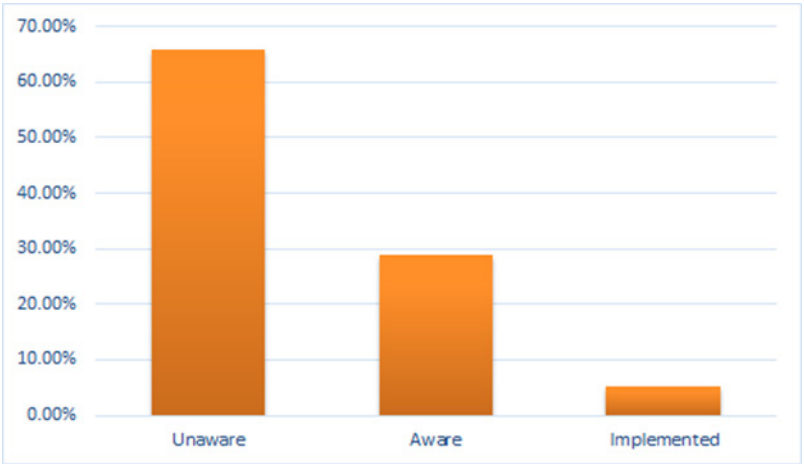


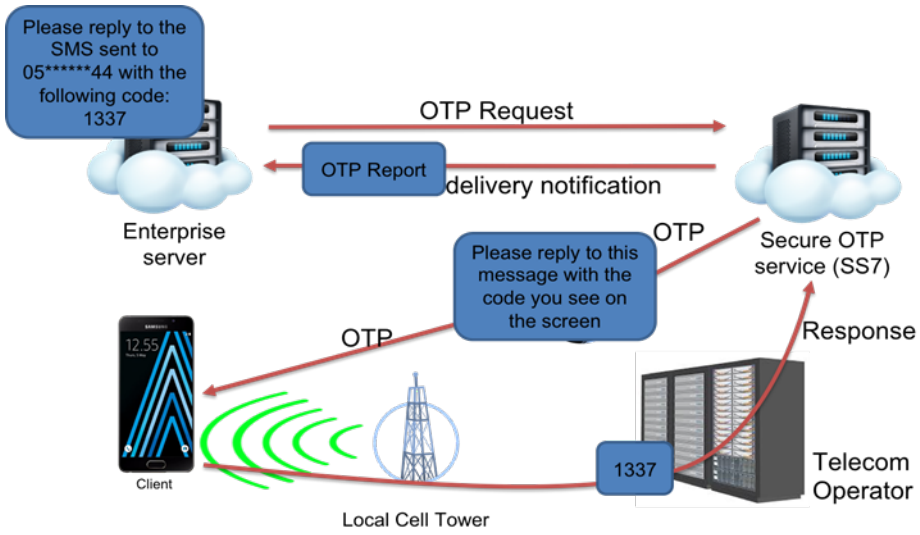
Figure 10 – La mise en œuvre des mesures d'atténuation des risques dans les pays en développement



mettre en place des mécanismes d'authentification et de chiffrement de premier ordre.

Toutefois, il existe de nombreux utilisateurs qui ne possèdent pas de smartphone et accèdent au DFS par la technologie USSD ou par SMS. Les recommandations et les stratégies évoquées plus haut permettent de contourner la plupart des attaques décrites dans ce document, mais seule une minorité d'opérateurs de réseau mobile à travers le monde a mis en œuvre des lignes directrices publiées par la GSMA. Dès lors, les fournisseurs de DFS victimes de fraude rencontrent des difficultés puisqu'ils ne sont pas en mesure d'empêcher ni d'atténuer les vulnérabilités auxquelles ils sont confrontés. Néanmoins, la connectivité SS7 leur permet de mettre en œuvre des stratégies d'atténuation des risques pour contrer les

Figure 11 – Détecter et limiter l'interception de SMS



attaques décrites plus haut. Voici quelques exemples de stratégies d'atténuation fondées sur la connectivité SS7 et qui ne nécessitent aucun investissement financier de la part de l'opérateur mobile.

12.1 Détecter et limiter les usurpations de compte fondées sur l'interception de mots de passe à usage unique envoyés par SMS

Pour détecter et limiter ces attaques, la procédure d'envoi du mot de passe à usage unique par SMS doit être abordée différemment. Le fournisseur de DFS doit mettre en place une procédure d'identification bidirectionnelle nécessitant, de la part de l'utilisateur, l'envoi (et non la réception) d'un mot de passe à usage unique. Ce processus consiste à afficher le mot de passe à usage unique dans une fenêtre quelconque (par exemple, une page Internet), puis à envoyer un SMS à l'utilisateur, qui devra répondre en renseignant le mot de passe affiché. Cette procédure permet au fournisseur de DFS de s'appuyer sur la technologie SS7 pour déterminer si l'envoi du SMS de réponse provient de l'utilisateur autorisé ou d'un attaquant. Pour cela, il lui suffit de consulter les métadonnées SCCP du SMS de réponse, d'authentifier l'appellation globale à l'origine de l'envoi et de vérifier que la localisation de l'utilisateur correspond à celle de son réseau domestique. La figure 11 illustre ce processus:

12.2 Détecter et limiter les attaques fondées sur l'ingénierie sociale et les messages USSD MT

Lorsqu'un attaquant demande à une victime de communiquer son numéro de compte et son code PIN, il essaie ensuite de renseigner ces informations depuis un autre téléphone afin d'enregistrer le nouvel appareil sur le compte de la victime et de transférer des fonds. Il peut également utiliser ces informations pour retirer des fonds depuis un guichet automatique bancaire (GAB), un commerce de proximité ou un kiosque (par exemple, un 7-Eleven).

Avant d'autoriser la transaction, le fournisseur de DFS doit vérifier les points suivants:

a) Vérifier que le téléphone de la personne titulaire du compte est localisé près du GAB ou du kiosque où la transaction a lieu (s'il s'agit d'une transaction sur GAB).
b) Obtenir les numéros IMSI et IMEI du téléphone à l'origine de la transaction afin de vérifier, auprès de l'opérateur de réseau mobile, que le détenteur du téléphone et du numéro IMSI est également le titulaire du compte.
c) Vérifier la légitimité de la transaction grâce à une procédure d'approbation bidirectionnelle avec envoi d'un mot de passe à usage unique (SecureOTP[12]) au numéro de téléphone original.

12.3 Détecter et limiter l'interception de transactions USSD réalisées depuis un terminal mobile

Un fraudeur qui réussit à intercepter le numéro de compte et le code PIN d'une victime tente ensuite

d'utiliser ces informations. Pour exploiter ces identifiants, il dispose principalement de deux options:

a) Pendant la session MITM, après avoir cloné la carte SIM de la victime grâce au système MITM, l'attaquant peut en profiter pour lancer une session USSD MO depuis ce système.
b) Après la session MITM, l'attaquant essaie ensuite de renseigner ces informations depuis un autre téléphone afin d'enregistrer le nouvel appareil sur le compte de la victime et de transférer des fonds (selon le mode opératoire décrit plus haut).

Nous allons maintenant nous concentrer sur la détection du premier cas de figure, étant donné que le second est identique au scénario décrit plus haut. Avant d'autoriser la transaction, le fournisseur de DFS doit vérifier les points suivants:

a) Vérifier que le numéro IMEI de l'appareil à l'origine de la transaction correspond bien au numéro IMEI pour le téléphone de la personne titulaire du compte (par un système d'attaque par interception, il est possible de cloner la carte SIM en utilisant un numéro IMEI différent).
b) Comparer la localisation du téléphone à l'origine de la transaction en cours à sa dernière localisation connue (dernier SMS ou appel entrant ou sortant): lorsqu'il est victime d'une attaque MITM, la localisation du réseau du téléphone change brusquement.

12.4 Détecter et limiter les échanges non autorisés de cartes SIM

Lorsque l'attaquant est en possession de la nouvelle carte SIM, il procède à la réinitialisation du code PIN grâce à l'envoi d'un mot de passe à usage unique par SMS. Avant d'autoriser la transaction, le fournisseur de DFS doit vérifier les points suivants:

a) Vérifier que le numéro IMSI associé au numéro de téléphone est resté le même. S'il a changé, cela pourrait indiquer un échange de carte SIM.
b) Dans ce cas, vérifier le numéro IMEI du téléphone associé à la carte SIM. S'il a changé également, cela indique une probabilité élevée d'échange de carte SIM. Dans ce cas, le fournisseur de DFS doit bloquer le compte en attendant de pouvoir procéder aux vérifications d'usage par l'intermédiaire d'un appel vocal ou d'un agent.
c) Pour détecter des comportements suspects indiquant une probabilité d'échange de carte SIM, des systèmes et des procédures peuvent être mis en place. Ils s'appuient, entre autres, sur les éléments suivants:

Une **réglementation** relative à l'échange de carte SIM, impliquant notamment les points suivants:

a) Les organismes de réglementation doivent imposer aux opérateurs de réseau mobile (MNO) et aux opérateurs de réseau virtuel mobile (MVNO) une réglementation normalisée en matière d'échange de carte SIM, y compris pour les échanges entraînant la portabilité d'un numéro vers un autre opérateur.
b) Toute personne demandant à recevoir une nouvelle carte SIM doit s'identifier auprès de son MNO, de son MVNO ou d'un agent. Lorsqu'il s'agit d'une demande par procuration, elle doit fournir une déclaration sous serment signée par l'abonné ainsi qu'une photo d'identité de ce dernier[13].
c) Lorsqu'il s'agit d'une demande de remplacement de carte SIM par procuration, le MNO, le MVNO ou l'agent doit procéder à la capture de l'image faciale du demandeur et conserver l'image pendant 12 mois[14].
d) La réglementation doit stipuler que seule peut faire l'objet d'un remplacement une carte SIM défectueuse, endommagée, volée, perdue, obsolète (mais éligible au remplacement ou à une mise à niveau) ou devenue inutilisable pour un motif raisonnable et légitime[15].

Une **réglementation interne** aux MNO et aux MVNO relative à l'échange de carte SIM, impliquant notamment les points suivants[16]:

a) Lorsqu'un échange de carte SIM est demandé, envoyer des notifications SMS, SVI ou USSD Push au détenteur (actuel) de la carte SIM et du numéro de téléphone, au cas où cette carte serait toujours active. Laisser ensuite un délai au détenteur pour confirmer la demande avant de procéder à l'échange de carte SIM.
b) Observer un délai d'attente de deux à quatre heures entre la demande d'échange de carte SIM et l'envoi de la nouvelle carte au demandeur.
c) Poser des questions de vérification à la personne qui est à l'origine de la demande d'échange de carte SIM, notamment la valeur du dernier bon de recharge prépayé utilisé et/ou les numéros de téléphone composés de manière régulière, ou

encore, en cas de facturation a posteriori, le nom de la personne ayant réglé la dernière facture.

d) Relier les bases de données de cartes SIM et de numéros de téléphone hébergées par les MNO aux systèmes d'authentification à deux facteurs utilisés par les banques ou les prestataires de services de paiement (PSP) pour vérifier l'identité du bénéficiaire par l'intermédiaire d'un mot de passe à usage unique envoyé par SMS et/ou par USSD Push. Cette mise en relation permettra à la banque ou au PSP d'effectuer des tests de vélocité afin de vérifier les demandes d'échange de carte SIM. Dès lors, il sera possible de signaler les demandes émanant d'un numéro lié au titulaire du compte, mais affichant une proximité temporelle suspecte avec une demande (potentiellement frauduleuse) d'ajout d'un nouveau bénéficiaire reçue par la banque ou le PSP.

12.5 Détecter, limiter et empêcher le recyclage de cartes SIM

Lorsqu'un compte de DFS reste inactif, il convient d'assurer un suivi de l'IMSI du numéro de téléphone associé au compte. Une fois la carte SIM désactivée, l'opérateur de réseau mobile ne pourra plus répondre correctement à ces requêtes (une requête par jour suffit pour assurer le suivi).

Lorsque la carte SIM est recyclée, l'opérateur de réseau mobile indique le nouvel IMSI du numéro de téléphone associé au compte. Le fournisseur de DFS doit alors bloquer temporairement le compte et vérifier que l'identité du nouveau détenteur de la carte SIM correspond bien à celle du titulaire du compte.

12.6 Intégration de données d'identification dans le téléphone de l'utilisateur à des fins d'authentification

Les fournisseurs de DFS peuvent collaborer avec les fabricants d'appareils et les MNO pour intégrer, dans le système d'exploitation de l'appareil, une information d'identification difficile à usurper. Cet identifiant (qui devra être chiffré pour contrer les tentatives d'usurpation) doit être intégré à l'ensemble des communications entre le fournisseur de DFS et l'utilisateur du téléphone, afin d'authentifier à la fois l'utilisateur et l'appareil.

12.7 Mesures de réglementation

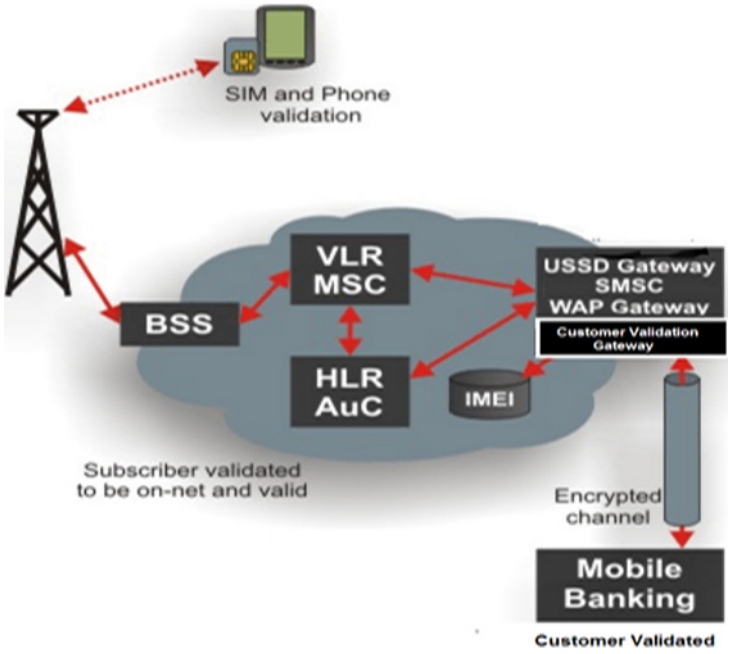
Les organismes de réglementation en charge des DFS peuvent mettre en place des procédures et des principes permettant la détection, la prévention, le signalement et l'atténuation des attaques SS7 et assimilées. Ils peuvent également mettre au point des procédures que les services détenteurs d'une licence devront mettre en œuvre pour empêcher l'échange de carte SIM.

La coordination réglementaire entre les organismes de réglementation concernés joue un rôle crucial dans la répartition des responsabilités et des fonctions communes ou spécifiques aux différents acteurs. Cette répartition doit faire l'objet d'un protocole d'accord entre les parties prenantes. L'annexe B propose un extrait d'un modèle de protocole d'accord entre un organisme de réglementation des télécommunications et une banque centrale, avec des tournures qui soulignent l'importance de ces responsabilités.

Entre autres sujets, le protocole d'accord évoque la nécessité d'attribuer à chaque organisme de réglementation des responsabilités techniques communes et spécifiques concernant les infrastructures et les problèmes de sécurité susceptibles d'affecter l'écosystème de DFS, notamment en matière de signalement et de lutte contre les intrusions. L'organisme de réglementation des télécommunications, en particulier, doit également collaborer avec les opérateurs détenteurs d'une licence pour mettre en œuvre une politique de tests réguliers permettant de détecter les intercepteurs d'IMSI. Le protocole d'accord envisage également la création d'un comité de travail conjoint permettant aux organismes de réglementation en charge des DFS et aux organismes en charge des télécommunications de se réunir une fois par mois pour discuter des enjeux relatifs aux DFS – et d'éventuelles menaces ou incidents auxquels ils sont exposés.

Pour confirmer que la technologie USSD est bien utilisée par des clients authentiques et enregistrés pour accéder à leurs systèmes, les fournisseurs de DFS et des banques ont la possibilité de recourir à une passerelle de validation par l'IMSI.

Figure 12 – Une passerelle de validation par l'IMSI



13 CONCLUSIONS ET RECOMMANDATIONS

Nous pouvons conclure que:

a) D'une manière générale, les fournisseurs de DFS, les opérateurs de télécommunications et les organismes de réglementation ne sont pas suffisamment informés des stratégies d'atténuation des risques dont ils disposent pour détecter et empêcher les attaques SS7.
b) Le faible taux d'exécution des mesures d'atténuation des risques s'explique principalement par l'absence d'une réglementation adéquate et par des coûts dissuasifs (pour l'opérateur de télécommunications).
c) Les attaques qui exploitent des vulnérabilités SS7 pour voler des fonds sont faciles à exécuter et ne sont pas l'apanage d'organismes gouvernementaux.
d) Pour les fournisseurs de DFS comme pour les opérateurs de réseau mobile, les mesures d'atténuation des risques prennent la forme de produits commerciaux prêts à l'emploi; avec une réglementation adéquate, ces deux catégories d'acteurs devraient donc être capables d'appliquer ces mesures.
e) Toutefois, en cas de fraude, les contrats actuels de DFS font peser l'entière responsabilité sur l'utilisateur final et les fournisseurs ne sont pas tenus d'indemniser la victime, ce qui ne les encourage pas à investir dans la résolution de ce type de problème.
f) Ce constat peut être étendu aux opérateurs de télécommunications: le préjudice financier causé par une fraude se limite au fournisseur de DFS et les opérateurs, qui ne peuvent être tenus pour responsables, ne subissent aucune perte et n'ont donc aucune raison d'investir leurs ressources dans la recherche d'une solution.
g) D'une manière générale, les autorités en charge des télécommunications et les banques centrales ont rarement – voire jamais – l'occasion de se rencontrer ou d'interagir pour dresser un état des lieux des intrusions et des menaces qui pèsent sur la sécurité des DFS.
h) Les membres de l'écosystème de DFS et les organismes de réglementation ont rarement – voire jamais – l'occasion de se rencontrer ou d'interagir dans un environnement neutre et collaboratif pour dresser ensemble un état des lieux des intrusions et des menaces qui pèsent sur la sécurité des DFS.

Pour régler les problèmes évoqués ci-dessus, le Groupe de travail recommande l'adoption des mesures suivantes:

a) **Éduquer les organismes de réglementation des télécommunications et des services financiers sur les vulnérabilités SS7 et leur impact sur les DFS** – Les organismes de réglementation des télécommunications et des services financiers du monde entier doivent avoir conscience de ces risques et, surtout, avoir conscience qu'il existe des solutions pour les atténuer.

b) **Mettre en place un cadre réglementaire et juridique comportant des mesures relatives à la sécurité de la signalisation et au signalement des incidents dans ce domaine** – Les organismes de réglementation des télécommunications et des services financiers doivent promulguer une réglementation pour obliger les fournisseurs de DFS et les opérateurs de télécommunications à mettre en œuvre des mesures d'atténuation des risques et à établir des rapports concernant les violations et les incidents de sécurité constatés.

c) **Établir des mesures de sécurité de base pour chaque catégorie de réseau (3G/4G/5G)** – Pour chaque catégorie de réseau (3G/4G/5G), les organismes de réglementation des télécommunications doivent établir des mesures de sécurité de base que les opérateurs devront ensuite mettre en œuvre afin de garantir un environnement d'interconnexion plus sûr.

d) **Établir une coordination sur le plan réglementaire** – Un protocole d'accord bilatéral relatif aux DFS doit être conclu entre les différents organismes de réglementation des télécommunications et les banques centrales correspondantes. Ce protocole d'accord doit prévoir les modalités d'instauration d'un comité de travail conjoint relatif à la sécurité des DFS et aux risques auxquels elle est exposée. L'annexe B propose un extrait de protocole d'accord qui pourra être utilisé comme modèle.

e) **Établir une coordination sur le plan de la réglementation sectorielle:** Des forums doivent être créés pour permettre à l'ensemble des acteurs commerciaux de l'écosystème de DFS de rencontrer les organismes de réglementation du secteur et d'interagir régulièrement avec eux dans un environnement neutre, afin de discuter librement des enjeux relatifs à la sécurité, sans pour autant divulguer aucune information sensible ou concurrentielle.

f) **Établir une coordination entre les différents acteurs du secteur:** Des forums doivent être créés pour permettre à l'ensemble des acteurs commerciaux de l'écosystème de DFS de se rencontrer et d'interagir régulièrement dans un environnement neutre, afin de discuter librement des enjeux relatifs à la sécurité, sans pour autant divulguer aucune information sensible ou concurrentielle, ni entreprendre aucune action susceptible d'entraver la libre concurrence.

g) **Encourager le secteur à agir** – Élaborer, en partenariat avec les acteurs du secteur, des programmes d'incitation permettant de favoriser le développement de mesures d'atténuation des risques en matière de fraude dans le domaine des télécommunications et des DFS.

h) **Encourager le secteur à agir** – Créer une réglementation destinée à inciter financièrement les fournisseurs de DFS et les opérateurs de télécommunications à agir en les obligeant à assumer la responsabilité du préjudice financier en cas de fraude.

ANNEXE A: DESCRIPTION TECHNIQUE DES PROTOCOLES SS7 ET DIAMETER

A.1 La pile de protocole SS7

Le système de signalisation n°7 (SS7) est un ensemble de protocoles de signalisation téléphonique développé en 1975 et utilisé pour l'établissement et la libération de la plupart des appels téléphoniques du réseau téléphonique public commuté (RTPC) à travers le monde. Le protocole SS7 permet également de proposer la traduction de numéros, la portabilité du numéro local, la facturation prépayée, l'envoi de messages courts (SMS) et d'autres services destinés au grand public.

En Amérique du Nord, il est souvent appelé CCSS7, pour "Common Channel Signaling System 7". Au Royaume-Uni, on parle de C7 ("CCITT number 7"), de numéro 7 et de CCIS7 ("Common Channel Interoffice Signaling 7"). En Allemagne, il s'agit du ZZK-7 ("Zentraler ZeichengabeKanal Nummer 7").

La série de recommandations Q.700, publiée en 1988 par l'UIT-T, a permis de mettre au point le seul protocole SS7 de portée internationale. La plupart des déclinaisons nationales s'inspirent de ce protocole international, tel qu'il a été fixé par l'ANSI et l'ETSI. Les déclinaisons nationales qui présentent les caractéristiques les plus frappantes sont les variantes chinoise et japonaise (TTC).

L'Internet Engineering Task Force (IETF) a mis au point l'ensemble de protocoles SIGTRAN, qui permet la mise en œuvre de protocoles de niveau 2, 3 et 4 compatibles avec le SS7. Également appelé Pseudo SS7, il est encapsulé dans le mécanisme de transport du SCTP.

La pile de protocole SS7 correspond en partie au modèle OSI de pile de protocole numérique par paquets. Les couches 1 à 3 du modèle OSI sont fournies par le sous-système de transport des messages (MTP) et le sous-système de commande des connexions sémaphores (SCCP) du protocole SS7 (le MTP et le SCCP forment ensemble le sous-système service de réseau (NSP)); pour les signalisations liées au circuit, comme le BT IUP, le sous-système utilisateur téléphonie (TUP) ou le sous-système utilisateur du RNIS (ISUP), la couche 7 est fournie par le sous-système utilisateur. À l'heure actuelle, aucune composante de protocole ne fournit les couches 4 à 6 du modèle OSI. Le sous-système gestionnaire de transactions (TCAP) est le principal utilisateur SCCP du réseau infrastructurel. Il utilise le mode sans connexion du SCCP. Le mode avec connexion du SCCP fournit une couche de transport pour les protocoles de l'interface radio tels que les protocoles BSSAP et RANAP. Le TCAP propose à ses utilisateurs des capacités de transaction, telles que le protocole MAP, le sous-système application de réseau intelligent (INAP) et le sous-système d'application CAMEL (CAP).

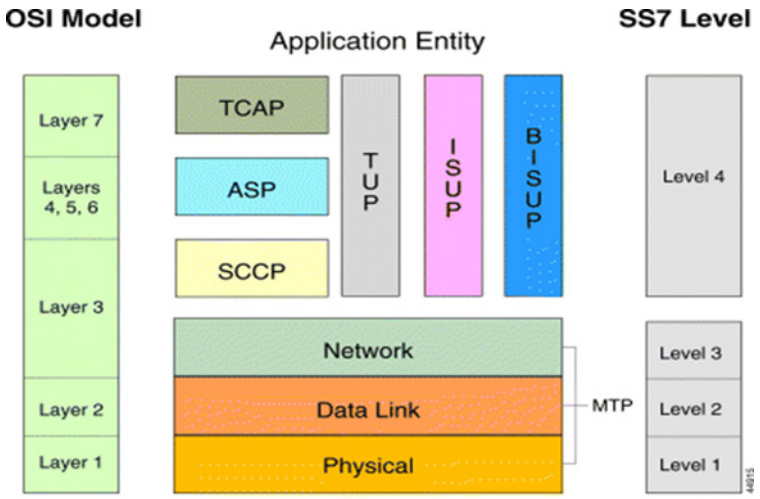
Le MTP couvre une partie des fonctionnalités de la couche réseau du modèle OSI, notamment: l'interface réseau, le transfert d'informations, la gestion des messages et le routage vers les niveaux supérieurs. Le SCCP correspond au niveau fonctionnel 4. Avec le MTP de niveau 3, il forme le NSP. Le SCCP complète les fonctionnalités de la couche réseau du modèle OSI: adressage et routage de bout en bout, messages sans connexion (UDT) et services de gestion pour les utilisateurs du NSP. Le TUP est un système de signalisation liaison par liaison utilisé pour connecter les appels. L'ISUP est une partie utilisateur dont le rôle est crucial, puisqu'elle fournit le protocole basé sur le circuit permettant d'établir, de maintenir et de mettre un terme aux connexions pour les appels. Le TCAP est utilisé pour créer des requêtes sur base de données et invoquer des fonctionnalités réseau avancées ou des liens vers l'INAP pour les réseaux intelligents et vers le MAP pour les services mobiles.

A.2 La pile de protocole Diameter

Le protocole Diameter est utilisé pour assurer la communication entre les différentes composantes de l'évolution de l'architecture système (SAE). La SAE correspond à l'architecture du réseau central pour la norme de communication sans fil LTE du 3GPP. Il s'agit d'une évolution du réseau central du GPRS, avec quelques différences:

- une architecture simplifiée;
- un réseau tout-IP;
- la prise en charge d'un débit plus élevé et une plus faible latence pour les réseaux d'accès radio;
- la prise en charge de multiples réseaux d'accès hétérogènes et la possibilité de passer de l'un à l'autre, notamment l'accès hertzien de terre universel évolué (l'interface radio du réseau LTE ou LTE Advanced), les systèmes hérités du 3GPP (par exemple GERAN ou UTRAN, les interfaces radio respectives du GPRS et de l'UMTS), ou encore les systèmes extérieurs au 3GPP (par exemple, le Wi-Fi, le WiMAX ou CDMA2000).

Figure A.1 – La pile de protocole SS7



La principale composante de l'architecture du SAE est le réseau central évolué en mode paquet (EPC), également connu sous l'appellation SAE Core. L'EPC assume les mêmes fonctions que les réseaux GPRS (par l'intermédiaire de l'entité de gestion de la mobilité, de la passerelle de desserte et des sous-composantes de la passerelle de réseau de données en mode paquet).

Les protocoles de la strate de non-accès (NAS) forment la strate la plus élevée du plan de contrôle entre l'équipement utilisateur et l'entité de gestion de la mobilité (MME). [3] Ils prennent en charge la mobilité de l'équipement utilisateur et les procédures de gestion de session destinées à établir et à maintenir la connectivité IP entre l'équipement utilisateur et la passerelle de réseau de données en mode paquet. Ces protocoles définissent les règles de mise en correspondance des paramètres en cas de mobilité inter-système entre les réseaux 3G et les réseaux d'accès non 3GPP. Ils contribuent également à la sécurité des protocoles NAS en assurant la protection de leur intégrité et le chiffrement des messages de signalisation NAS. Le système évolué en mode paquets (EPS) fournit à l'abonné une connectivité IP "prête à l'emploi" et une expérience "toujours disponible" en assurant la liaison entre la gestion de la mobilité et la gestion de session pendant les procédures d'enregistrement de l'UE.

Les transactions NAS complètes consistent en une série de procédures élémentaires spécifiques, qui s'appuient sur des protocoles de gestion de la mobilité du système EPS (EMM) et de gestion des session EPS (ESM).

A.3 La pile de protocole EPC

A.3.1 Protocoles MME

La pile de protocole MME est composée de:

- La pile S1-MME pour la prise en charge de l'interface S1-MME avec le nœud B évolué;
- La pile S11 pour la prise en charge de l'interface S11 avec la passerelle de desserte (SGW).

La MME prend en charge l'interface S1 avec le nœud B évolué. La pile de l'interface intégrée S1-MME est composée des protocoles IP, SCTP et d'application pour l'interface S1 (S1AP).

- Le protocole SCTP est un protocole de transport répandu, qui utilise les services du protocole IP pour proposer un service fiable de transmission de datagrammes aux modules d'adaptation tels que le protocole S1AP. Le protocole SCTP offre une transmission fiable et séquencée, qui s'ajoute au cadre IP existant. Les principales fonctionnalités proposées par le protocole SCTP sont:

  i) La mise en place d'une association: une association est une connexion établie entre deux terminaux à des fins de transfert de données, sur le modèle d'une connexion TCP. Une association SCTP permet de spécifier des adresses multiples pour chaque terminal.
  ii) La fiabilité de la transmission des données: transmission de flux de données séquencées (élimination des blocages en tête de ligne). Le protocole SCTP permet de garantir la

transmission de données séquencées sous la forme de flux unidirectionnels multiples et d'éviter le blocage de morceaux de données transmises dans l'autre sens.

- S1AP est le service de signalisation entre le réseau d'accès hertzien de Terre universel évolué et l'EPC, qui permet de remplir les fonctionnalités de l'interface S1, telles que la gestion du support SAE, le transfert du contexte initial, la mobilité de l'équipement utilisateur, la pagination, la réinitialisation, le transport de signalisation NAS, les rapports d'erreurs, la libération du contexte de l'équipement utilisateur, le transfert de statut.

La MME prend en charge l'interface S11 avec la SGW. La pile de l'interface intégrée S11-MME se compose des protocoles IP, de datagramme d'utilisateur (UDP) et GTP-C évolué (eGTP-C).

A.3.2 Protocoles SGW

La SGW se définit comme suit:

- La pile de plan de contrôle S11 pour la prise en charge de l'interface S11 avec la MME;
- Les piles de plan de contrôle et de plan de données S5/S8 pour la prise en charge de l'interface S5/S8 avec la passerelle de réseau de données à commutation par paquets (PGW);
- La pile de plan de données S1 pour la prise en charge de l'interface du plan utilisateur S1 avec le nœud B évolué;
- La pile de plan de données S4 pour la prise en charge de l'interface du plan utilisateur S4 entre le contrôleur de réseau d'accès radioélectrique de l'UMTS et le SGW du nœud B évolué;
- Sxa: depuis la publication de sa quatorzième "release", l'interface Sx et le protocole PFCP associé ont été ajoutés au PGW, permettant ainsi la séparation du plan de contrôle et du plan utilisateur entre PGW-C et PGW-U;
- La SGW prend en charge l'interface S11 avec la MME et l'interface S5/S8 avec la PGW. La pile de plan de contrôle intégrée pour ces interfaces se compose des protocoles IP, UDP et eGTP-C.

Le SGW prend en charge l'interface S1-U avec le nœud B évolué et l'interface du plan de contrôle S5/S8 avec la PGW. La pile de plan de données intégrée pour ces interfaces se compose des protocoles IP, UDP et eGTP-U.

A.3.3 Protocoles de passerelle de réseau de données en mode paquet

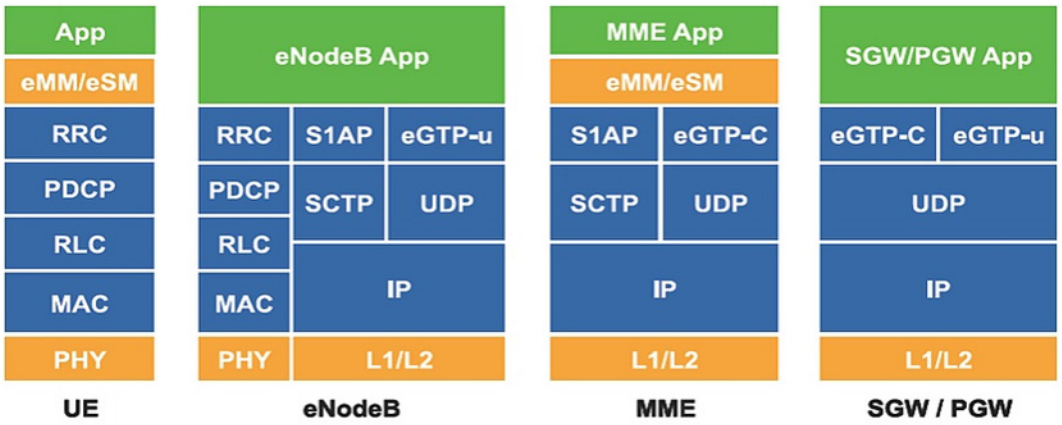
Les principales interfaces prises en charge par la PGW sont les suivantes:

- S5/S8: cette interface se situe entre la SGW et la PGW. On l'appelle S5 lorsque la SGW et la PGW sont situées dans le même réseau (scénario sans itinérance) et S8 lorsque la SGW est située dans le réseau visité et la PGW dans le réseau domestique (scénario avec itinérance). L'interface S5/S8 utilise les protocoles eGTP-C et GTP-U.
- Gz: cette interface est utilisée par la PGW pour communiquer avec le système de facturation hors-ligne (OFCS), principalement pour les relevés de données de facturation (CDR) des utilisateurs facturés a posteriori, envoyés par l'intermédiaire du protocole de transfert de fichiers (FTP).
- Gy: cette interface est utilisée par la PGW pour communiquer avec le système de facturation en ligne (OCS). La PGW informe en temps réel l'OCS des montants facturés aux utilisateurs prépayés. L'interface Gy utilise le protocole Diameter.
- Gx: cette interface est utilisée par la PGW pour communiquer avec la fonction des règles relatives à la politique et à la taxation (PCRF) pour la gestion des règles de contrôle de la politique et de la taxation (PCC). Ces règles comportent des éléments relatifs à la facturation, ainsi que des paramètres de qualité de service qui seront appliqués par l'établissement du détenteur. L'interface Gx utilise le protocole Diameter.
- SGi: cette interface se situe entre la PGW et les réseaux externes, tels que l'accès à Internet, l'accès à l'intranet d'entreprise, etc.
- Sxb: depuis la publication de sa quatorzième version, l'interface Sx et le protocole PFCP associé ont été ajoutés au PGW, permettant ainsi la séparation du plan de contrôle et du plan utilisateur entre PGW-C et PGW-U.

A.4 Prise en charge des services vocaux et des SMS

L'EPC est un réseau central fonctionnant exclusivement par paquets. Il ne dispose pas d'un domaine de commutation de circuits tel que ceux utilisés traditionnellement pour les communications téléphoniques vocales et SMS.

Figure A.2 – La pile de protocole LTE (Diameter)



A.4.1 Solutions issues des spécifications 3GPP dans le domaine de la téléphonie

- Sous-sytème multimédia IP (IMS): Parmi les spécifications de la septième version du 3GPP, on trouve notamment l'IMS pour la voix sur IP.
- Repli de commutation de circuits (CSFB): pour émettre ou recevoir des appels, l'équipement utilisateur change de technologie d'accès radio et passe de la technologie LTE à la technologie 2G/3G, qui prend en charge les services de commutation de circuits. Cette fonctionnalité nécessite une couverture 2G ou 3G. Elle nécessite également l'établissement d'une nouvelle interface (baptisée SGs) entre le protocole MME et le diagramme de séquences de messages (MSC). Cette fonctionnalité a été développée dans la huitième version du 3GPP.

A.4.2 Solutions issues des spécifications 3GPP dans le domaine des SMS

- IMS: Parmi les spécifications de la septième version du 3GPP, on trouve notamment l'IMS pour les SMS sur IP.
- SMS sur SGs: cette solution nécessite l'emploi de l'interface SGs, introduite pendant l'exécution du CSFB. Les SMS sont acheminés par la technologie LTE vers la strate de non-accès. Aucune modification inter-système n'est nécessaire pour l'émission ou la réception de SMS. La spécification de cette fonctionnalité fait partie de la huitième version.
- SMS sur SGd: cette solution nécessite l'emploi de l'interface Diameter SGd sur le MME et consiste à envoyer les SMS sur la strate de non-accès par l'intermédiaire de la technologie LTE, sans passer par une signalisation complète, qu'il s'agisse du CSFB exécuté par le MSC hérité ou du préfixe associé à la signalisation de l'IMS et à la gestion du support EPC.

Le CSFB et les SMS sur SGs sont considérés comme des solutions temporaires, contrairement à l'IMS, plus durable.

ANNEXE B : MODÈLE POUR UN PROTOCOLE D'ACCORD ENTRE L'ORGANISME DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS ET LA BANQUE CENTRALE SUR LA SÉCURITÉ DES DFS

B.1 FONDEMENTS DU PROTOCOLE D'ACCORD

En reconnaissance de la convergence croissante des services de télécommunications et des services financiers au sein d'entités communes désignées par l'appellation "services financiers numériques" (DFS), les autorités ont identifié des besoins en matière d'interaction et de collaboration entre les différents organismes de réglementation, afin de garantir l'intégrité, la sécurité, la stabilité et la protection des parties prenantes et des utilisateurs finaux qui fournissent ou bénéficient de ces services.

La BANQUE CENTRALE et l'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS doivent coopérer pour assurer le contrôle et la surveillance des fournisseurs de DFS et des réseaux de communication des MNO – dans le respect de leurs mandats respectifs, tant sur le plan financier que sur le plan des télécommunications – de manière à garantir le plus haut degré d'exigence possible en matière de sécurité, de fiabilité, de protection des usagers, d'équité d'accès aux équipements et de confidentialité.

Par ailleurs, en reconnaissance du fait que la BANQUE CENTRALE et l'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS disposent chacun d'un champ limité en matière de contrôle et de surveillance des composantes des DFS, le présent protocole d'accord vise à établir des modalités communes de supervision et d'interaction sur les enjeux relatifs aux DFS inscrits dans les prérogatives et les mandats respectifs des deux autorités signataires, qui s'engagent ainsi à renforcer le cadre de réglementation, de contrôle et de surveillance des DFS en/au/aux/à [nom du pays] et à combler d'éventuelles lacunes.

Ce protocole d'accord est signé sur la base d'un respect mutuel, dans un esprit de bonne volonté et n'affecte en rien l'indépendance des deux autorités signataires.

Ce protocole d'accord vise à favoriser l'intégrité, l'efficience et l'efficacité des parties prenantes en optimisant la réglementation et en renforçant la supervision des DFS.

B.2 DOMAINES ET STRATÉGIES DE COOPÉRATION

DISPOSITIONS GÉNÉRALES

B.2.1 Les parties signataires acceptent de coopérer, en conformité avec leurs rôles respectifs, sur le traitement des enjeux suivants:

a) Les DFS en général;
b) L'accessibilité, l'équité d'accès, la sécurité et la fiabilité de l'ensemble des composantes des DFS en/au/aux/à [nom du pays];
c) La protection des usagers;
d) Tout autre domaine de collaboration possible entre les deux autorités signataires.

B.2.2 La coopération entre la BANQUE CENTRALE et l'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS se concentrera sur les enjeux et les processus suivants:

a) L'échange d'informations utiles;
b) Le renforcement mutuel des capacités;
c) L'ouverture d'une enquête en cas d'incident, de problème ou de situation relevant du champ d'application du présent protocole d'accord;
d) L'organisation d'auditions conjointes ou individuelles, selon les besoins;
e) L'utilisation de systèmes communs pour le suivi des transactions effectuées depuis les DFS;
f) L'action en faveur du respect de la concurrence et de l'égalité des chances pour toutes les parties prenantes de l'écosystème de DFS;
g) La résolution de conflits entre les fournisseurs et les utilisateurs finaux;
h) L'élaboration, le suivi et l'application, dans les lois, les réglementations et les directives, de dispositions relatives aux DFS;
i) Des consultations destinées à proposer, pour les différentes lois, réglementations et directives existantes, des amendements relatifs aux DFS;
j) Des consultations destinées à proposer de nouvelles lois, réglementations et directives relatives aux DFS;
k) Le recours à une expertise technique;
l) La gestion et l'exploitation de l'infrastructure de DFS;
m) La disponibilité des canaux de communication des opérateurs de réseau mobile (MNO) et l'équité d'accès pour tous les fournisseurs de DFS;

n) La disponibilité et l'équité d'accès pour les données des MNO juridiquement éligibles à une diffusion auprès des fournisseurs de DFS ou d'autres parties;
o) L'élaboration et l'application des normes techniques et opérationnelles minimales;
p) L'identification, l'atténuation, le traitement rapide et la maîtrise de l'ensemble des problèmes et incidents de sécurité;
q) Lorsque cela est nécessaire, la participation à l'élaboration des cadres de gestion des risques relatifs aux DFS;
r) Lutte contre le blanchiment d'argent, le financement du terrorisme et la fraude;
s) La protection générale des usagers;
t) La surveillance des systèmes et des réseaux à des fins de détection des violations de la sécurité et des intrusions susceptibles d'affecter les DFS, et leur signalement à l'autre autorité signataire;
u) Le soutien aux activités de l'autre autorité signataire relatives aux DFS et aux sujets connexes;
v) Le signalement rapide à l'autre autorité signataire de l'ensemble des problèmes, des processus et des événements susceptibles d'affecter le fonctionnement des DFS en/au/aux/à [nom du pays];
w) Toute autre stratégie entrant dans le champ d'application du présent protocole d'accord et jugée nécessaire et appropriée par les deux autorités signataire.

FONCTIONS ASSIGNÉES À L'AUTORITÉ NATIONALE DES TÉLÉCOMMUNICATIONS

B.2.3 L'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS doit assurer la surveillance continue des fréquences agréées exploitées par les MNO, de façon à garantir qu'aucun appareil à radiofréquence non autorisé ne soit utilisé sur lesdites fréquences pour, entre autres, intercepter des informations sur les usagers ou perturber les communications entre les MNO et leurs abonnés.

Si nécessaire, cette surveillance peut être assurée conjointement par l'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS et les MNO. Toute intrusion ou violation susceptible d'affecter l'exploitation et la sécurité financière des DFS en/au [nom du pays] doit être signalée dans les meilleurs délais par l'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS à la BANQUE CENTRALE.

B.2.4 Dans le cadre de son mandat de surveillance et de supervision, l'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS agira pour garantir que les opérateurs détenteurs d'une licence offrent leurs services aux fournisseurs de DFS:

a) À un niveau technique élevé;
b) À un niveau de sécurité élevé;
c) À un niveau de disponibilité élevé pour garantir aux usagers des communications et/ou des transferts de données sans interruption;
d) De manière efficace et abordable;
e) De manière juste et équitable;
f) Sans abuser de la licence qui leur a été accordée pour l'exploitation des ressources de télécommunications et sans tirer avantage de la quantité limitée desdites ressources au détriment d'autres entités dont le fonctionnement en dépend;
g) De manière transparente;
h) Sans opérer de distinction entre les différents fournisseurs de DFS ni entre les autres entités dont le fonctionnement dépend de ces ressources, que ce soit en matière de coût, d'accessibilité ou de qualité de service;
i) Sans retarder l'acheminement et la transmission d'aucun message de service;
j) Dans le respect des droits de propriété intellectuelle;
k) Tout en garantissant la disponibilité de l'accès au réseau selon les normes en vigueur;
l) Sans nuire au principe de libre concurrence;
m) Lorsque les détenteurs de la licence sont des MNO, ils doivent s'assurer que seules les personnes authentifiées et autorisées sont en mesure d'accéder aux cartes SIM des usagers – ou, le cas échéant, d'en fournir;
n) Selon les besoins, s'assurer que les opérateurs mettent en œuvre une politique constante de test, de filtrage des intrus et de surveillance des réseaux centraux, de l'infrastructure des stations d'émission-réception de base et des bandes de fréquences de téléphonie mobile agréées afin d'empêcher d'éventuelles tentatives d'accès, de perturbation ou d'utilisation non autorisées.

B.2.5 La surveillance et les tests relatifs aux questions spécifiées dans la section 2.4 ci-dessus et qu'il sera nécessaire, le cas échéant, de mettre en œuvre portent notamment, mais pas exclusivement, sur les points suivants:

a) L'accès non autorisé et l'usage de toute composante centrale de l'infrastructure d'un MNO basée sur l'ensemble de protocoles SS7;
b) L'usage de toute composante SS7 de l'infrastructure d'un MNO à des fins d'activité non autorisée ou frauduleuse;
c) L'accès non autorisé et l'usage de toute composante centrale de l'infrastructure d'un MNO basée sur la norme LTE;
d) Dans la mesure du possible et en fonction des capacités techniques, la détection des appareils à radiofréquence non autorisés exploités par des acteurs non autorisés et susceptibles d'être conçus pour perturber les activités des MNO détenteurs d'une licence et/ou pour accéder frauduleusement au téléphone fixe, à la carte SIM et aux données des usagers, ainsi qu'à leurs droits d'accès aux équipements de MNO et de DFS.

B.2.6 L'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS doit également s'assurer que les opérateurs détenteurs d'une licence et l'ensemble des entités qu'il supervise:

a) Transmettent à l'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS des rapports relatifs aux tests de pénétration liés à la sécurité de leurs systèmes. Le cas échéant, ces rapports doivent notamment mentionner les actions correctives entreprises;
b) Transmettent à l'ORGANISME NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS des rapports relatifs aux incidents liés aux autorisations d'accès à leurs systèmes et à leurs données. Ces rapports doivent notamment mentionner les pertes de données et les violations des mesures de protection des données des usagers, qu'elles soient effectives ou potentielles, ainsi que les actions correctives entreprises;
c) Appliquent dans les meilleurs délais les normes internationales les plus récentes en matière de technique et de sécurité;
d) Offrent aux utilisateurs finaux des DFS le plein accès aux différents fournisseurs de DFS et la possibilité de choisir, sans aucune restriction, discrimination ni traitement de faveur.

FONCTIONS ASSIGNÉES À LA BANQUE CENTRALE

B.2.7 La BANQUE CENTRALE doit assurer la surveillance constante des entités qu'elle supervise.

B.2.8 Dans le cadre de son mandat de surveillance et de supervision, la BANQUE CENTRALE agira pour garantir que les opérateurs détenteurs d'une licence et les entités qu'elle supervise:

a) Offrent leurs services aux fournisseurs de DFS:

   i) À un niveau technique élevé;
   ii) À un niveau de sécurité élevé;
   iii) À un niveau de disponibilité élevé pour garantir aux usagers des communications et/ou des transferts de données sans interruption;
   iv) De manière efficace et abordable;
   v) De manière juste et équitable;
   vi) Sans abuser de la licence ou de l'autorisation d'exploitation qui leur a été accordée au détriment d'autres entités dont le fonctionnement dépend des ressources concernées;
   vii) De manière transparente;
   viii) Sans opérer de distinction entre les différents fournisseurs de DFS, que ce soit en matière de coût, d'accessibilité ou de qualité de service;
   ix) Sans retarder l'acheminement et la transmission d'aucun message de service;
   x) Dans le respect des droits de propriété intellectuelle;
   xi) Tout en garantissant la disponibilité de l'accès au service selon les normes en vigueur.

b) Ne nuisent pas au principe de libre concurrence;
c) Selon des besoins, mettent en œuvre une politique constante de test, de filtrage des intrus et de surveillance des infrastructures afin d'empêcher d'éventuelles tentatives d'accès, de perturbation ou d'utilisation non autorisées; et, dans les meilleurs délais:

   i. Transmettent à la BANQUE CENTRALE des rapports relatifs aux tests de pénétration liés à la sécurité de leurs systèmes. Le cas échéant, ces rapports doivent notamment mentionner les actions correctives entreprises;
   ii. Transmettent à la BANQUE CENTRALE des rapports relatifs aux incidents liés aux autorisations d'accès à leurs systèmes et à leurs données. Ces rapports doivent notamment mentionner les pertes de données et les

violations des mesures de protection des données des usagers, qu'elles soient effectives ou potentielles, ainsi que les actions correctives entreprises;

iii. Appliquent les normes internationales les plus récentes en matière de technique et de sécurité;

d) Offrent aux usagers des DFS la possibilité de choisir entre différents fournisseurs, sans aucune restriction, discrimination ni traitement de faveur.

Notes de fin

1 L'annexe A présente la pile de protocole SS7 sous forme de diagramme.

2 L'annexe A présente la pile de protocole Diameter sous forme de diagramme.

3 Les résultats de l'enquête menée par l'ENISA peuvent être consultés (en anglais) à l'adresse suivante: .

4 Reference: https://www.gsma.com/newsroom/gsmadocuments/technical-documents/

5 Ce constat repose sur une série d'audits récents menés par Vaulto sur plus d'une vingtaine de réseaux mobiles.

7 Update Location – une opération SS7 qui induit en erreur le réseau domestique de la victime en simulant son itinérance vers un autre réseau.

8 Enregistreur de localisation des visiteurs

9 https://mwnation.com/be-alert-mobile-money-fraudsters-on-the-loose/

10 Le routage domestique des SMS évite que l'IMSI réelle d'un abonné ne soit communiquée avec chaque signalisation de SMS entrant. Toutefois, la signalisation peut subir d'autres types d'attaques qui permettent d'extraire l'IMSI du registre HLR de l'opérateur de télécommunications.

11 En théorie, le filtrage au niveau des nœuds de signalisation permet d'interdire l'accès depuis une adresse non vérifiée. Toutefois, cette méthode n'est efficace que si le filtrage est correctement configuré et maintenu.

12 Procédure bidirectionnelle d'envoi d'un mot de passe à usage unique par SMS permettant d'éviter les attaques par interception.

13 Nigerian Communications Commission (2017), Directives relatives au remplacement d'une carte SIM, disponible à l'adresse suivante (en anglais): https://www.ncc.gov.ng/docman-main/legal-regulatory/guidelines/733-guidelines-on-sim-replacement/file

14 Nigerian Communications Commission (2017), Directives relatives au remplacement d'une carte SIM, disponible à l'adresse suivante (en anglais): https://www.ncc.gov.ng/docman-main/legal-regulatory/guidelines/733-guidelines-on-sim-replacement/file

15 Nigerian Communications Commission (2017), Directives relatives au remplacement d'une carte SIM, disponible à l'adresse suivante (en anglais): https://www.ncc.gov.ng/docman-main/legal-regulatory/guidelines/733-guidelines-on-sim-replacement/file

16 Cette réglementation peut s'inspirer des lignes directrices proposées par l'organisme de réglementation en matière d'échange de carte SIM.

Union internationale des télécommunications (UIT)
Place des Nations
CH-1211 Genève 20
Suisse