Chapitre 11

La Sécurité dans les Réseaux Mobiles de Télécommunication

11.1. Introduction

Les réseaux de télécommunications commutés par circuits (réseaux de téléphonie) ont été créés à une époque de forte tendance monopolistique des compagnies d'états. Selon les pays, soit l'opérateur du service était contrôlé par l'état, soit l'opérateur était une compagnie privée en position de monopole. Le but essentiel était l'accomplissement de la tâche de service public, à savoir l'établissement de communications téléphoniques sur le territoire. L'accès à la structure du réseau s'effectuait par des liens filaires analogiques pour lesquels l'identité de l'usager, sa localisation et son adresse de facturation étaient confondues. Les collaborations inter-réseaux nécessaires à un service d'appel mondial reposaient sur des accords mutuels basés sur la réputation des acteurs. Les réseaux cellulaires de première génération ont repris en grande partie ces principes de base.

Avec l'arrivée des réseaux cellulaires de radiotéléphonie numérique (tels que le GSM), la faille potentielle provenant de l'accès radio, les compagnies ont donc requis une authentification formelle sécurisée des clients. En revanche, aucune forme d'authentification sécurisée n'était jugée nécessaire de la part des compagnies vis-à-vis des clients étant donné qu'ils étaient opérateur unique sur un territoire et que le prix des équipements nécessaires à usurper un opérateur national était jugé dissuasif.

Un changement majeur dans la vision de la sécurité des réseaux est apparu après la dérégulation des télécommunications. En effet, la loi a permis, et même força dans certains cas (loi anti-trust des Etats-Unis), l'émergence d'opérateurs alternatifs ou simplement virtuels, louant dans un premier temps les infrastructures de

---

Chapitre rédigé par Jérôme Härri et Chrisitian Bonnet.

transmissions de l'opérateur historique. De nouveaux défis apparurent à ce moment là. En effet, avec l'apparition de nouveaux entrants dans l'arène des télécommunications, la sécurisation par réputation n'était plus suffisante. De plus, avec des opérateurs virtuels louant les infrastructures des opérateurs, la question du contrôle de la facturation est devenue cruciale.
Le réseau Sémaphore 7 (SS7) est le réseau de signalisation des réseaux publics commutés (RTC) dans le monde entier. Le réseau SS7 est commuté par paquets, et il est physiquement séparé du réseau RTC afin d'accélérer le temps d'établissement des circuits ainsi que pour lutter contre les fraudes. Par la situation monopolistique des opérateurs de télécommunications, leur accès contrôlé au réseau SS7 était la seule mesure de sécurité afin de lutter contre les fraudes. Jusqu'à ces dernières années, cette mesure fut jugée suffisante. Cependant, avec l'interconnexion et la dérégulation des réseaux, le contrôle centralisé d'accès a cessé d'être satisfaisant, sans que de nouvelles mesures de sécurité soient ajoutées.
Avec la dérégulation, les opérateurs ont aussi commencé à devoir proposer des services innovants afin de se distinguer de la concurrence. Ces nouveaux services ont reposé dans un premier temps sur le concept de « *réseau intelligent (IN)* » capables de gérer l'interopérabilité ainsi que l'hétérogénéité des technologies d'accès. Certains services étant à fort potentiel économique (portabilité des numéros, numéros verts, numéros azurs), la sécurisation des données du réseau IN devint aussi un sujet de débat.
Une évolution supplémentaire provint de l'interconnexion des réseaux de télécommunications avec le réseau Internet. Cela a eu de multiples conséquences sur les opérateurs alternatifs ou virtuels, dont la principale fut le dégroupage de l'accès filaire téléphonique, et par là du réseau SS7, pour l'accès aux réseaux de télécommunication. Il devint aussi possible pour les opérateurs de téléphonie cellulaire d'offrir un accès mobile à Internet et à des opérateurs Internet s'offrir des services comme l'envoi de SMS vers des mobiles. De plus, de nouvelles techniques d'accès aux réseaux de télécommunications venues de l'Internet ont permis de lutter contre des lacunes sécuritaires avérées.
Des lors, une collaboration fructueuse se créa entre les réseaux fixes, mobiles, et le réseau Internet. Les deux premiers bénéficiant d'une transmission de données plus rapide et le dernier profitant d'une connexion locale pour ses services. Le service Internet qui apparut en concurrence directe avec les opérateurs fixes et mobiles fut la transmission de voix par paquets, appelé VoIP. Cette nouvelle application, avec d'autres liées à des applications multimédia, seront traitées en détail dans le chapitre consacré aux réseaux de nouvelle génération.

Dans ce chapitre, notre but est d'illustrer les mécanismes de sécurité employés dans les réseaux mobiles de télécommunication, ainsi que d'exposer les failles et les solutions qui ont été proposées afin d'assurer aux opérateurs ainsi qu'aux clients une exploitation sécurisée de leur données et infrastructures. En revanche, notre but n'est pas de répertorier les attaques avérées ou envisageables, mais simplement d'aborder les types d'attaque ainsi que les méthodes pouvant exploiter à des fins illégales les failles de sécurités des réseaux mobiles de télécommunications.

11.2. Signalisation

La signalisation dans les réseaux de télécommunications a toujours été le point névralgique du bon fonctionnement d'un réseau. En effet, c'est à travers une signalisation fiable que des appels sont acheminés correctement à la bonne destination, ou que le service souscrit est facturé à la bonne personne. Le corollaire de ce fait est que la signalisation a, dès le début, été sujet à des tentatives de sabotage de la part de groupes de personnes désirant profiter d'un réseau de télécommunication, ou plus inquiétant, visant à son détournement ou sa mise hors service. Par ce fait, il est très important de développer des protocoles de signalisation robustes et le cas échéant, identifier ses failles afin de les corriger.

Durant l'automne 1997, le réseau de télécommunication de Porto Rico a été saboté en coupant physiquement des lignes de communications. Avec la convergence des mondes de l'information et des télécommunications, et notamment l'interconnexion des divers réseaux de communications, il devient aussi possible de mener une attaque similaire à distance en attaquant les réseaux de signalisations. Nous allons identifier et décrire dans cette section des attaques moderne utilisant les failles de signalisations des protocoles SS7.

Bien que le problème de signalisation ne soit pas particulier aux réseaux de télécommunications mobiles, le fait que tous reposent sur SS7 ou un autre système de signalisation plus complexe fait que la sécurisation de la signalisation est un facteur important dans la sécurité des systèmes de télécommunication mobiles.

11.2.1. Signalisation Sémaphore 7 (SS7)

Le protocole de signalisation majeur utilisé dans les réseaux de communications est la **Signalisation Sémaphore 7 (SS7)**. Il est employé que ce soit dans des réseaux publics commutés, les réseaux cellulaires et même dans l'interconnexion avec les réseaux IP. Sa diffusion est mondiale comme est celle de sa pile de protocole et de sont fonctionnement, ce qui ouvre aussi la porte a des attaques visant ses failles. Le réseau SS7 permet de faire dialoguer entre eux les équipements du réseau de communication tels que commutateurs, base de données d'abonnés etc.

L'architecture SS7 consiste en un réseau haut débit commuté par paquets. Il a été crée afin de se superposer et gérer la signalisation des réseaux. Le réseau SS7 peut dès lors être employé indépendamment par des réseaux commutés par paquets ou par circuits. Comme illustre par la Figure 1, ce réseau consiste en une interconnexion entre trois types de liens de signalisations communément appelés nœuds SS7 :

- *Service Switching Point (SSP)* : Il agit au nom des commutateurs qui sont origine, ou destination d'un appel. Un SSP envoie de la signalisation afin de configurer, gérer et relâcher des circuits de communication nécessaires à un appel. Il peut aussi effectuer une requête auprès du SCP afin d'obtenir des informations sur l'appel.
- *Service Control Point (SCP)* : Il déclenche la mise en oeuvre d'une base de donnée regroupant les informations pour gérer des services de communications avancés, comme les numéros vert, les cartes d'appel prépayés et le nomadisme. Ces bases de données représentent l'intelligence du service et sont au cœur de l'approche « réseau intelligent » (IN)
- *Signal Transfer Point (STP)* : Un STP est un point de commutation intermédiaire qui achemine chaque message de signalisation à sa destination basé sur les informations contenu dans la trame SS7. Un STP fonctionne aussi comme un pare-feux et scrute les messages SS7 reçu de réseaux externes.

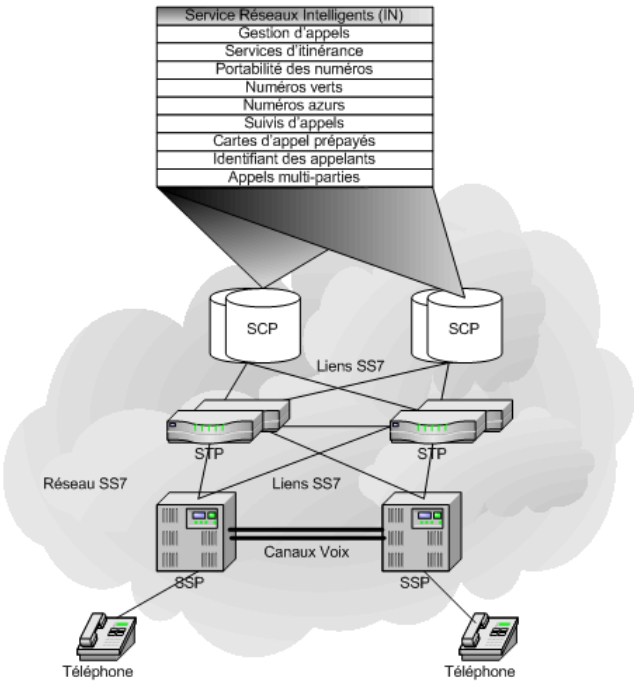


Figure 1 *Architecture SS7*

Chaque nation a un plan d'adressage propre pour ses nœuds SS7. L'interconnexion mondiale des réseaux de signalisation est réalisée au travers de certains nœuds particulier qui possèdent également une adresse internationale et qui agissent comme passerelle.
Le réseau SS7 étant critique au bon fonctionnement de la gestion des appels, les SCP ainsi que les STP sont déployés en configuration paritaire dans des lieux différents afin de parer à des pannes locales. La résilience des réseaux face à des attaques et des pannes est basée sur la confidentialité de la structure du réseau et non sur la sécurité du protocole en lui-même.

SS7 concerne la signalisation échangée entre les équipements d'un réseau de télécommunication.
En ce qui concerne la signalisation entre le terminal utilisateur et le premier élément de réseau (un commutateur), une signalisation spécifique d'accès existe. Dans le cas d'un poste utilisateur numérique (au standard RNIS – Réseau Numérique à Intégration de Services) un protocole spécifique pour l'établissement des communications est mis en place avec le commutateur. C'est sur ce principe que le GSM a bâti le protocole d'accès entre un terminal mobile et le réseau d'infrastructure.

La relative sécurité de SS7 est provenue de la faible pénétration externe des réseaux propriétaires de télécommunication. Cependant, après la dérégulation des télécommunications, de nouveaux acteurs sont entrés sur le marché. Les plus connus en Europe sont les nouveaux opérateurs alternatifs de communications, mais aussi les opérateurs de télécommunications mobiles virtuelles (MVNO). L'autorité de régulation des télécommunications les autorise, pour des sommes modiques, à se connecter à un réseau SS7 ou d'interconnecter leur petit réseau SS7 à un plus grand afin d'élargir l'offre. Comme l'illustre la Figure 2, ce qui était auparavant un grand nuage SS7 faiblement interconnecté est devenu un réseau de réseaux SS7 fortement interconnectés et imbriqués. Le point commun à cela est que les réseaux ne sont plus dignes de confiance sans autre forme de protection. Le contrôle d'accès à son propre réseau SS7 devient donc une très grande priorité afin d'éviter l'utilisation ou la reconfiguration frauduleuse des nœuds SS7.

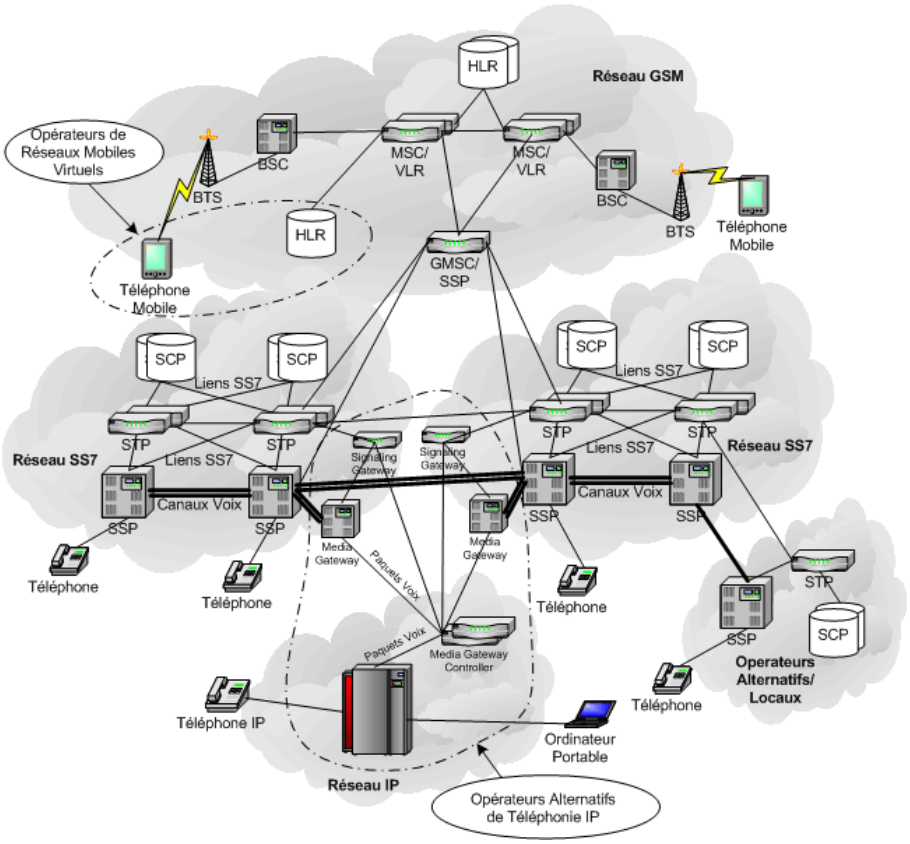


Figure 2 *Interconnexion des réseaux*

11.2.2. La pile de protocole SS7

La pile de protocoles SS7 est composée de quatre niveaux. Les trois premiers ont la charge d'assurer des transferts point à point alors que le quatrième niveau représente la partie applicative de SS7. La Figure 3 illustre la pile de protocole SS7.

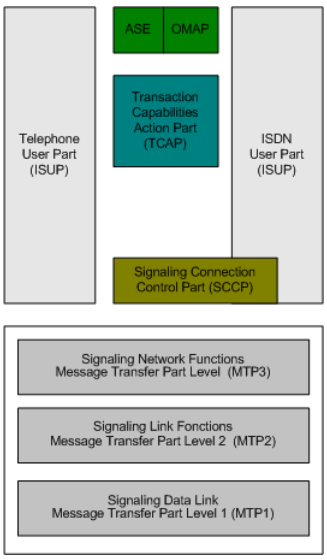


Figure 3 *Pile de protocoles SS7*

La pile de protocoles SS7 consiste en sept fonctions principales

- *Signaling Data Link (MTP1)* : Il définit la couche physique de SS7.
- *Signaling Link Functions (MTP2)* : Il s'agit de la couche de lien assurant la fiabilité des transmissions.
- *Signaling Network Functions (MTP3)* : Cette couche achemine les messages entre les SSP de point à point. Elle assure aussi une répartition homogène du trafic entre les SSP, ou redirige les liens si une liaison est tombée.
- *Signaling Connection Control Part* (SCCP) : Cette couche étend le MTP en incluant des fonctions avancées de routage comme la traduction des titres globaux (numéraux verts, numéro d'appel global de cartes prépayées) en adresse de SSP, et assure le transport de services orienté connexion ou non. Contrairement à MTP, SCCP assure une connexion de bout en bout.
- *Transaction Capabilities Application Part (TCAP)* : Permet d'échanger des données entre des applications à travers SS7 en utilisant la version non orientée connexion de SCCP. Les transactions entre les SCP et les STP s'effectuent avec TCAP. Dans les réseaux mobiles comme le GSM, les messages MAP, échangés entre des infrastructures et les bases de données, sont aussi acheminés par TCAP.

- *Telephone User Part (TUP)* : Il définit les fonctions internationales de signalisation d'établissement de communication. Il ne permet pas l'établissement de liens de données.
- *ISDN User Part (ISUP)* : Définit le protocole utilisé afin de configurer, gérer et relâcher des circuits de voix ou de données entre SSP. ISUP est utilisé pour des appels ISDN ou non-ISDN.

11.2.3. La vulnérabilité des réseaux SS7

Comme mentionné précédemment, la plus grande vulnérabilité des réseaux SS7 est le manque de contrôle d'accès. En effet, quiconque étant capable de générer des messages SS7 et de les introduire dans un réseau SS7, peut perturber les services de l'opérateur. Par exemple, la perturbation du suivi d'appel d'un opérateur peut créer un véritable chaos dans l'acheminement d'appels. Sur la Figure 4, nous mettons en évidence trois intrusions potentielles sur un réseau SS7.

Premièrement, des utilisateurs possédant des téléphones RNIS peuvent introduire des messages sur le réseau SS7 via l'interface d'accès utilisateur. Par exemple, *l'attaquant 1* peut usurper l'identité du téléphone source et introduire des paquets malveillants dans le réseau.

Une seconde vulnérabilité provient de la convergence des réseaux de télécommunications avec Internet. En effet, elle donne la possibilité à *un attaquant 2* de pénétrer le réseau SS7. De larges portions d'Internet louent les réseaux de télécommunications fixes, et inversement, les réseaux SS7 sont interconnectés grâce à Internet. En conséquence, les réseaux SS7 deviennent vulnérables aux failles d'Internet, et les failles des réseaux SS7 peuvent perturber, à leur tour, Internet. Finalement, alors que les réseaux propriétaires sont relativement protégés, cela n'est pas le cas des opérateurs alternatifs. En conséquence, un attaquant peut pénétrer le réseau principal en compromettant les ordinateurs du réseau alternatif (*attaque 3*).

Il est à noter que l'accès à un réseau SS7 par des réseaux mobiles, virtuels ou non, est actuellement considéré comme sécurisé pour les réseaux GSM et GPRS. Cependant, la dérégulation des télécommunications mobiles apporte aussi son lot de vulnérabilités et ces réseaux pourraient aussi devenir de possibles sources d'attaques.

Une autre faille significative provient du service de portabilité des numéros de téléphone entre les opérateurs. Ce service autorise les clients à changer d'opérateurs tout en conservant leur numéro de téléphone initial. Malheureusement, une fois qu'un attaquant a réussi à pénétrer un réseau SS7, il devient virtuellement impossible de contrer ses attaques.

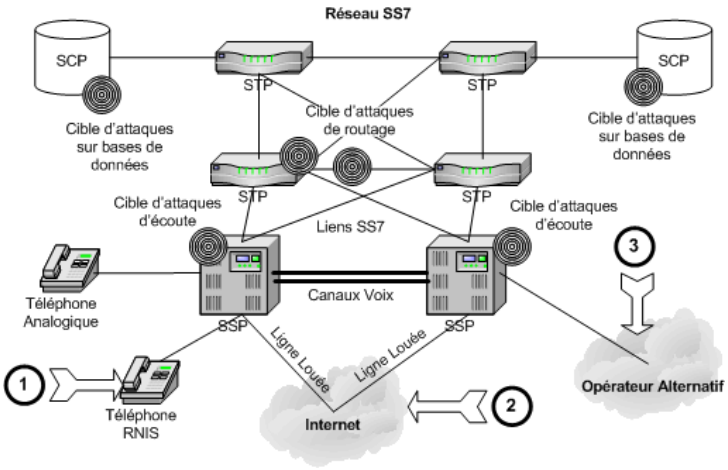


Figure 4 *Exemples d'attaques sur SS7*

11.2.4. Les attaques possibles sur les réseaux SS7

Les failles du réseau SS7 abordées dans la section précédente donnent naissance à une pléthore d'attaques possibles classifiées comme *modification*, *interception*, *interruption et mensonge*. Leurs cibles sont les trois types de nœuds SS7 comme illustré sur la Figure 4.

- *Attaque sur les SSP* : Les nœuds SSP font partie du périmètre du réseau SS7 et font donc office de passerelles d'attaque. Notamment, ils sont particulièrement sujets aux « sniffing » d'un utilisateur car son trafic total passe par son nœuds SSP dédié. D'autres attaques utilisent simplement le manque de contrôle d'accès sur l'interface utilisateur. Par exemple, le protocole RNIS a été créé afin d'autoriser l'accès direct au réseau SS7 par le téléphone numérique.
- *Attaque sur les STP* : Les nœuds STP étant au coeur du routage dans les réseaux de télécommunication basés sur SS7, des attaques perturbant l'acheminement des paquets de signalisation est potentiellement très néfaste. Par exemple, le trafic SSP passe directement par les STP. Leur compromission permet donc d'observer le trafic en provenance et à destination des SSP correspondants. Il est aussi possible de modifier le filtrage STP et de ré-acheminer le trafic, permettant donc d'écouter les communications.
- *Attaque sur les SCP* : Les nœuds SCP stockent des informations sensibles pour le système de signalisation et sont donc très vulnérables. Par exemple, prenons le cas des numéros verts. Les numéros verts cachent le numéro

réellement composé. En fait, le vrai numéro est échangé durant la phase de signalisation et si un utilisateur frauduleux parvient à pénétrer le SCP et à échanger le vrai numéro de téléphone lié au numéro vert, il lui deviendra possible de téléphoner gratuitement. Des modifications similaires sont possibles concernant, par exemple, les données de facturations, les données de portabilité des numéros, ou les données d'information sur la ligne téléphonique d'un utilisateur. Il devient donc possible d'usurper l'identité d'un client ou de téléphoner à moindres frais.

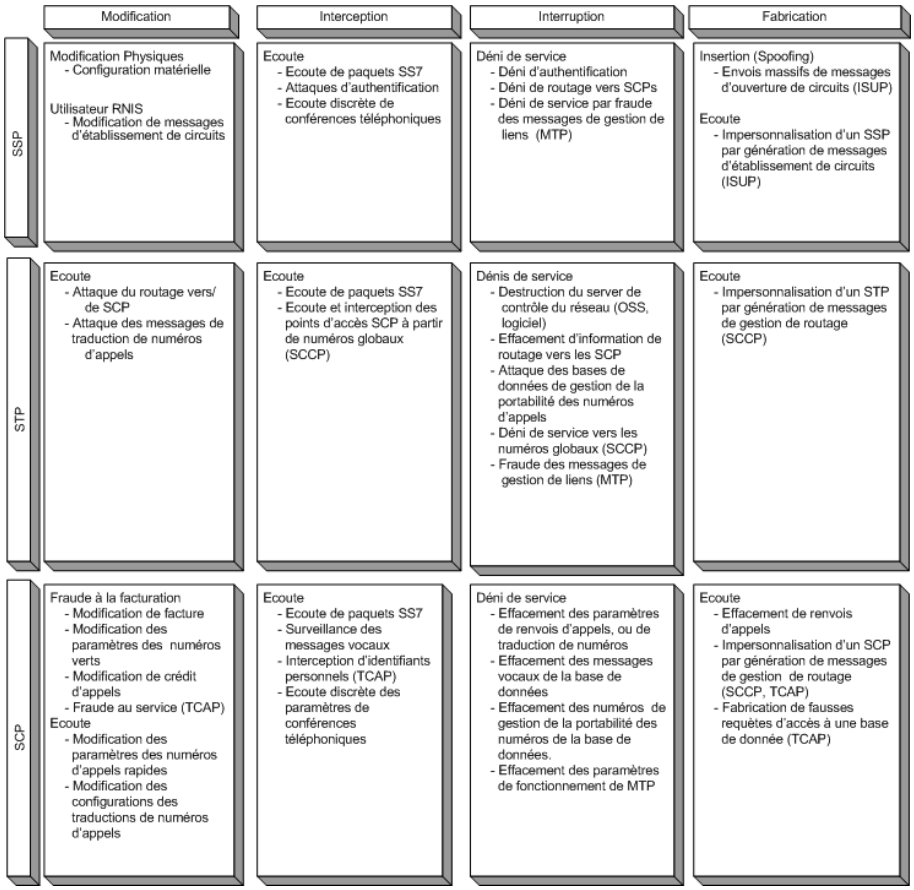


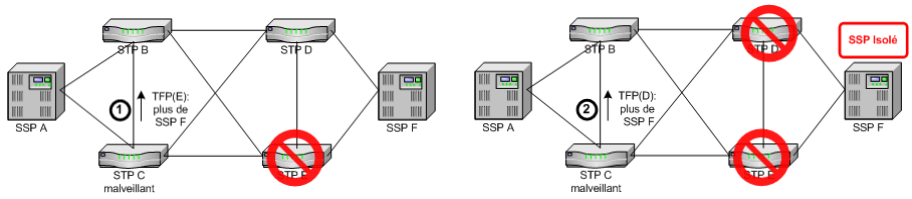
Figure 5 *Taxonomie d'attaques sur SS7*

11.2.5. Sécuriser SS7

Afin de tenter de sécuriser SS7, les opérateurs doivent parvenir à contrôler l'accès au réseau SS7 ainsi que le comportement des nœuds. SS7 n'ayant pas été pensé pour gérer des comportements malicieux, la situation rend très difficile, voire impossible, la lutte contre toutes les formes d'attaques possibles sur SS7. Une solution est donc de lutter en priorité contre les attaques à fort potentiel de perturbation.
Parmi toutes les attaques possibles répertoriées sur la Figure 5, les attaques sur la couche MTP sont minoritaires. Cependant, elles ont la capacité de complètement bloquer un réseau SS7. Dès l'apparition des premiers rapports illustrant ces problèmes, les industriels ont développé des rustines. Telcordia's *Gateway Screening* [TEL 01] contrôle les en-têtes des messages MTP3 de la pile SS7, équivalente à la couche réseau de la pile OSI. Le système est capable de vérifier de manière plus approfondie les messages de maintenance réseau SS7, ainsi que de vérifier que les points d'accès d'origine et de destination sont valides. Cependant, ce système ne peut pas contrôler le contenu des messages situés plus haut dans la pile SS7. Tekelec's *EAGLE STP Gateway Screening (GWS)* [TEK 01] est similaire à la solution de Telcordia, mais fournit un contrôle de messages à la couche MTP et à la couche SCCP. Une autre solution plus ambitieuse est Verizon's SS7 *Security Gateway Keeper* [VER 02] qui inclut aussi le contrôle d'ordonnancement, de syntaxe, et de contenu.

Principalement, toutes les solutions proposées sont des pare-feux pour le réseau SS7, qui pâtissent des limitations bien connues de ce genre de sécurité. L'absence de contrôle d'authentification et d'intégrité dans les réseaux SS7 reste un facteur majeur dans l'apparition d'attaque comme l'isolement d'un point d'accès voire d'une partie de réseau, ou la modification de l'acheminement vers un nœud malveillant. Nous illustrons dans la Figure 6, un exemple d'attaque en deux phases, premièrement effectuant une diversion de trafic, et ensuite en isolant un SSP. Cette attaque profite de l'absence de contrôle d'intégrité dans les messages TFP (TransFer Prohibited), qui sont employé en principe afin de prévenir les éléments du réseau qu'un lien est tombé. Si un intrus impersonnalise un STP (dans notre exemple, le STP D et E), il parvient donc à envoyer des faux messages TFP et à perturber le réseau.

Une solution a été proposée, appelée *MTPSec* [SEN 05], permettant une sécurisation de liens à liens sur le réseau SS7, et même la sécurisation des liens d'interconnexion entre deux réseaux SS7. En effet, MTPSec propose d'encrypter les communications sur les liens MTPs afin d'assurer l'intégrité des messages et donc de supprimer certaines perturbations d'acheminement dans le réseau SS7. Si cette approche est augmentée d'une solution basée sur un pare-feu, cela pourrait non seulement limiter les accès mais aussi les comportements malicieux.



Modification de routage SS7 ***Isolement d'un noeud SS7***

Figure 6 *Attaque sur le routage SS7*

D'autres solutions propriétaires ou académiques ont été proposées afin de pouvoir détecter des attaques sur SS7, ou d'empêcher une intrusion [LOR 01]. Notamment, il a été proposé de créer un système de contrôle au niveau applicatif appelé *Security Application Part (SecAP)* [SEI 98] qui coordonne diverses plateformes de contrôle distribuées dans le réseau SS7, comme un pare-feux sur les STP, un contrôle d'accès sur les SSP ainsi que sur les SCP.

11. 3. Sécurité dans le monde GSM

En 1982, le groupe de travail appelé le Groupe Spécial Mobile (GSM) fut crée par la Conférence Européenne des administrations des Postes et Télécommunications (CEPT). Son but fut la création d'une norme numérique de seconde génération pour la téléphonie mobile. Elle fut mise au point par l'ETSI sur les gammes de fréquence des 900 MHz et 1800MHz. Cette norme a connu un succès fulgurant qui a assuré une utilisation en Europe, Afrique, au Moyen Orient et en Asie. Les Etats-Unis, qui n'ont pas cru initialement au système, ont développé tardivement une version sur la gamme de fréquence des 1900Mhz. Vingt ans après sa création, la technologie GSM couvre 95% des nations mondiales et dépasse les 500 millions d'utilisateurs. Tel qu'il a été créé, le système GSM est particulièrement efficace pour les communications basées sur la voix, et similairement aux lignes fixes, il utilise la commutation de circuit. Afin de joindre un réseau GSM, un utilisateur a le choix entre prendre un abonnement ou acheter une carte d'appel prépayée.

11.3.1. Architecture GSM

Le réseau spécifique pour le GSM est appelé le RMT (Réseau Mobile Terrestre) et chaque opérateur non virtuel a le sien. Récemment, de nombreux d'opérateurs virtuels louant les structures d'un RMT ont fait leur apparition. Le GSM est finalement relié au réseau téléphonique commute public (RTC). Pour plus d'information relative au réseau GSM, le lecteur peut se référer à [GSM 01].

Comme illustré sur la Figure 7, un réseau RMT est composé de 4 grandes entités :

- *Une station mobile (MS)* qui est un téléphone mobile, bien qu'en règle générale, n'importe quel appareil disposant d'un transmetteur adéquat et d'une carte SIM (*Subscriber Identity Module*) peut faire office de station mobile.
- *Le sous-système station de base* (BSS), qui est composé d'un réseau de relais radio *Base Transceiver Stations (BTS)* et de leurs concentrateurs *Base Station Controller (BSC)*. Les BTS émettent et captent les signaux à destination et en provenance des stations mobiles. Il s'agit de la seule interface radio de tout le système GSM. En effet, la communication entre les BTS et le BSC ainsi que dans le reste du réseau se fait par lien numérique filaire basé sur la signalisation SS7.
- *Le sous-système réseau (NSS)*, qui a la charge du routage approprié des appels entre deux utilisateurs du réseau ou vers l'extérieur. Il est composé de commutateurs spécialisés *Mobile Switching Centers (MSC)* reliés entre eux et qui ont la charge de plusieurs BSC. A chaque MSC est associé une base de données *Visitor Location Register (VLR)* gérant les informations des abonnés se trouvant dans la zone radio gérée par le MSC. Une base de données unique, bien que distribuée afin de limiter les risques, le *Home Location Register (HLR)*, gère les informations des abonnés de l'opérateur du réseau. Le HLR contient aussi l'*Authentification Center* (AuC) qui a la charge de l'identification des utilisateurs. La contre partie des informations de l'AuC se trouvent dans la carte SIM de l'abonné. Des copies locales d'informations sont effectuées entre les HLR et les VLRs afin d'accélérer le traitement des requêtes du MSC. Un MSC particulier appelé *Gateway MSC (GMSC)* se trouve au point d'entrée du réseau de l'opérateur mobile et assure donc la passerelle avec le réseau téléphonique commuté (RTC).
- La partie Opération et Maintenance, est gérée par *l'Operation and Maintenance Center (OMC)* qui est en charge de veiller au bon fonctionnement de tous les systèmes du GSM.

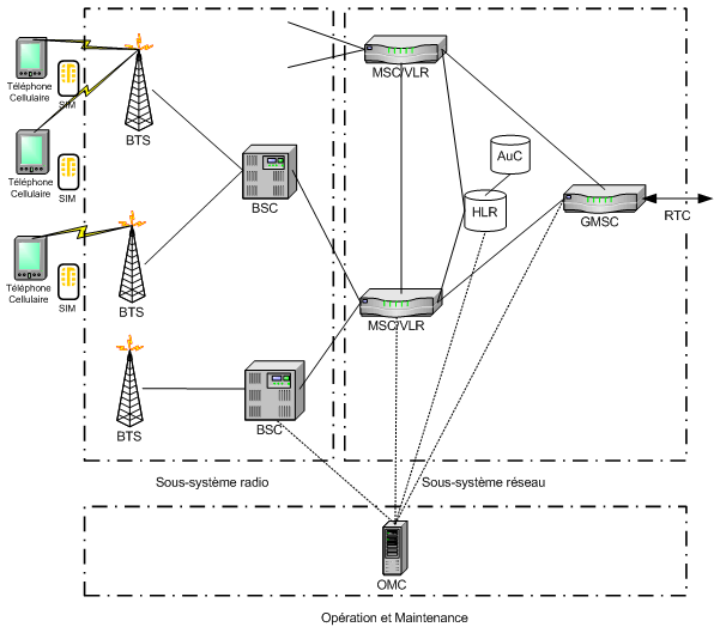


Figure 7 *Architecture GSM*

11.3.1.1. GSM et le Réseau Sémaphore 7

Comme mentionné auparavant, la signalisation ainsi que la commutation de circuits dans le NSS est basée sur SS7. Cependant, GSM ayant des besoins particuliers notamment en terme d'itinérance, ainsi que d'accès aux plateformes de réseau intelligent (IN), deux nouveaux protocoles majeurs ont été créé pour la collaboration entre SS7 et les réseaux GSM et sont illustré sur la Figure 8.

- *Mobile Application Part (MAP)* : Il s'agit d'un protocole qui fournit une communication au niveau applicatif entre les différents nœuds dans le NSS GSM. Il est, entre autre, chargé de l'acheminement des SMS, ou de la gestion de la mobilité et de l'itinérance. Il doit donc échanger des informations entre les VLR/HLR appartenants à différents réseaux de télécommunications cellulaires.
- *Customized Applications for Mobile network Enhanced Logic (CAMEL)*: Il permet l'interconnexion des réseaux mobiles aux plateformes IN. Il assure donc aux usagers un accès à des services, comme des *communications prépayées*, *la portabilité du numéro*, ou des *applications localisées*. Le protocole utilisé est le *CAMEL Application Part (CAP).*

Ces deux protocoles (MAP/CAP) sont aussi présents dans le GPRS, l'UMTS et IMS.

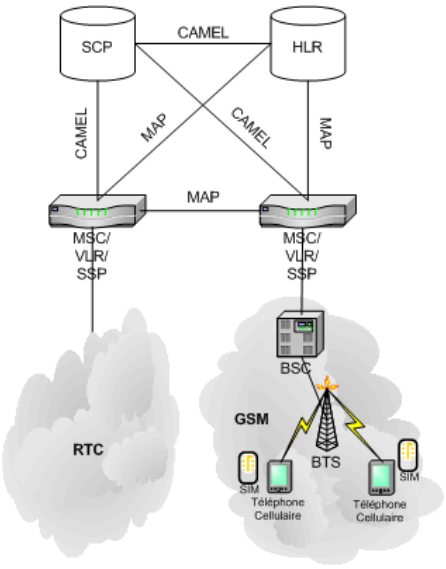


Figure 8 *Architecture MAC/CAP*

11.3.2. Mécanismes de Sécurité dans le GSM

Les protections de sécurité offertes par le système GSM actuel sont principalement restreintes à la protection d'accès au réseau de l'opérateur et au chiffrement radio. L'émergence de mécanismes sécuritaires supplémentaires relevants de la sécurité applicative est relativement récente. Il s'agit de mécanismes de protections de messages échangés entre la carte SIM et un serveur applicatif. En revanche, le NSS est considéré comme fiable. Dans cette section, nous allons donc uniquement aborder la sécurisation du lien radio et le contrôle d'accès.

La sécurité dans le GSM est composée de trois protections

- *Protection de l'identité de l'abonné*. En effet, il est dangereux de transmettre l'identité d'un abonné en clair sur un lien radio pour des raisons de confidentialité.
- *Contrôle d'accès au réseau* grâce à la carte SIM. La principale fonction du *Subscriber Indentity Module (SIM)* est de contenir, et de générer, une série d'informations confidentielles afin que le réseau puisse identifier avec certitude l'identité de l'utilisateur. La Figure 9 illustre les informations contenues dans une puce SIM nécessaires au fonctionnement du GSM.

- *Chiffrement des communications radio* entre la station mobile et la station de base. L'écoute de communications radio étant plus aisée que celle sur des liens filaires, il devient donc important de protéger le lien radio.

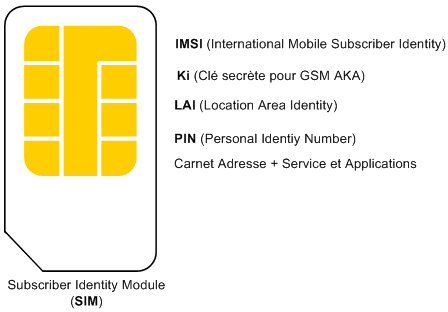


Figure 9 *Données contenues dans une puce SIM*

11.3.2.1. La protection de l'identité de l'utilisateur

Le principe de cette fonction est d'empêcher la divulgation de quel utilisateur utilise quelle ressource dans le réseau en écoutant le trafic de signalisation sur le lien radio. Cela a premièrement pour but d'assurer la confidentialité des données et du trafic de signalisation. Deuxièmement, cela doit aussi empêcher la localisation et le suivit d'une station mobile. Cela veut donc dire qu'en aucun cas, le numéro international de l'utilisateur (IMSI) contenu dans la carte SIM ainsi que dans le HLR doit être transmis en clair.
A la place, le système utilise un numéro d'utilisateur temporaire (TMSI) sur le lien radio. Le TMSI est temporaire et n'a qu'une validité locale, ce qui signifie qu'uniquement le regroupement du TMSI avec l'identifiant de la zone locale (LAI) permet de retrouver l'IMSI. L'association entre l'IMSI et le TMSI est gardée dans le VLR qui a aussi la charge de générer un nouveau TMSI lors d'un nomadisme hors de la zone locale.
La Figure 10 illustre le mécanisme d'échange dans le but qu'un mobile puisse obtenir un nouveau TMSI. L'identité de l'utilisateur est donc protégée par deux méthodes. La première, en ne transmettant qu'un ancien TMSI sur le lien radio, et le second en chiffrant le nouveau TMSI. Il y a cependant une faille à ce système comme nous le verrons dans la prochaine section.

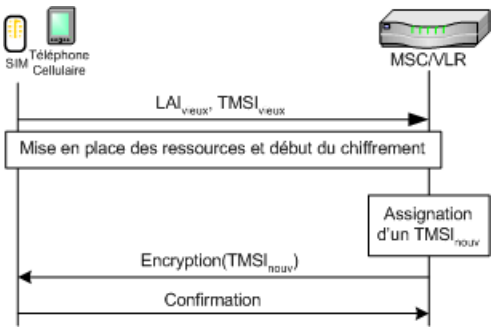


Figure 10 *Protection de l'identité d'un utilisateur dans le GSM*

11.3.2.2. Le contrôle d'accès

Lorsqu'un nouvel utilisateur est ajouté au réseau, une clé secrète d'authentification d'utilisateur (K_i) est aussi assignée en addition de l'IMSI afin de vérifier l'identité de l'utilisateur. Tous les mécanismes de sécurités sont basés sur le secret de cette clé. Elle ne doit absolument jamais ni être transmise, ni être compromise. Cette clé est gardée par le réseau dans l'AuC du réseau d'origine, et par l'utilisateur dans la carte SIM.
L'authentification utilise donc cette clé symétrique. Cette approche est due principalement aux limitations technologiques des cartes à puce du début des années 90. Comme illustré par la Figure 11, le processus d'authentification est basé sur l'algorithme A3 exécuté par le processeur de la carte SIM. A3 calcule de manière indépendante à partir d'un nombre aléatoire (RAND) et la clé secrète K_i une réponse (SRES). Le mobile renvoie cette réponse SRES au réseau. Si cette réponse est identique à la réponse attendue SRES, alors l'identité de l'utilisateur est vérifiée. A chaque exécution de l'algorithme, la valeur aléatoire est modifiée afin d'éviter le rejeu même si les communications radio sont écoutées.

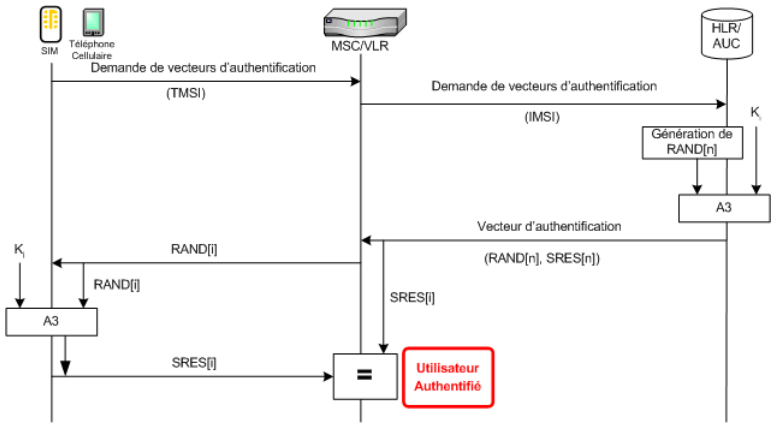


Figure 11 *GSM AKA*

Le duplet (RAND, SRES) est généré dans l'AuC par l'algorithme A3 à chaque fois qu'une authentification est nécessaire. Afin d'accélérer le processus, l'AuC peut calculer par avance des vecteur de duplets ($RAND_i$, $SRES_i$).
Plusieurs algorithmes A3 existent dont l'utilisation dépend de l'opérateur. Cependant, étant donné que le vecteur d'authentification est généré par l'AuC du réseau d'origine, l'authentification en itinérance reste assurée.

11.3.2.3. Chiffrement des communications radio

Le chiffrement des communications radio est une caractéristique particulière des réseaux GSM qui les différencient des réseaux analogiques de première génération et RNIS. Ce chiffrement, uniquement à la demande du BSC, est effectué sur la couche physique de transmission après le codage canal et l'entrelacement mais avant la modulation ce qui peut ajouter de la redondance dans le message chiffré et simplifier la cryptanalyse du chiffrement.
Une clé de chiffrement K_c est générée par le réseau et le mobile en utilisant l'algorithme A8 de la carte SIM et de l'AuC à partir de la clé secrète K_i et du nombre aléatoire (RAND) (voir Figure 12). Cette clé est ensuite utilisée pour l'algorithme de chiffrement A5 par la station mobile et la station de base (BTS). Il existe plusieurs versions de l'algorithme A5 (A5/1, A5/2, A5/3) dont l'utilisation dépend du pays. L'algorithme A5/3 est en faite l'algorithme KASUMI qui est aussi implémenté dans l'UMTS, cependant avec une longueur de clé de seulement 64 bits et des paramètres d'entrées simplifiés. Le réseau calcule la clé K_c dans l'AuC et génère donc un triplet (RAND, SRES, K_c) qui peut être utilisé à la demande.

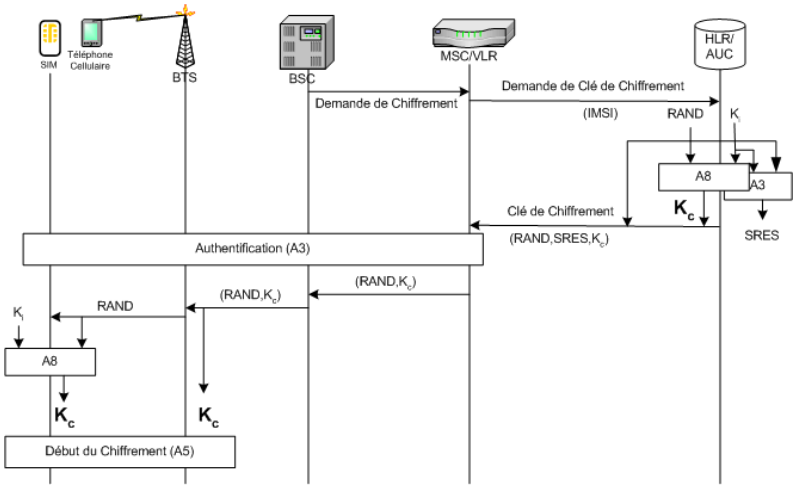


Figure 12 *Génération de la clé de chiffrement GSM*

Le chiffrement proprement dit est effectué par le mobile et la station de base. Il est utilisé afin de sécuriser les données utilisateur ainsi que le trafic de signalisation. Etant donné qu'il s'agit d'un cryptage symétrique, le cryptage et décryptage est effectué avec la même clef K_c et l'algorithme A5. La Figure 13 schématise la mise en place du chiffrement GSM entre un utilisateur et la station de base.

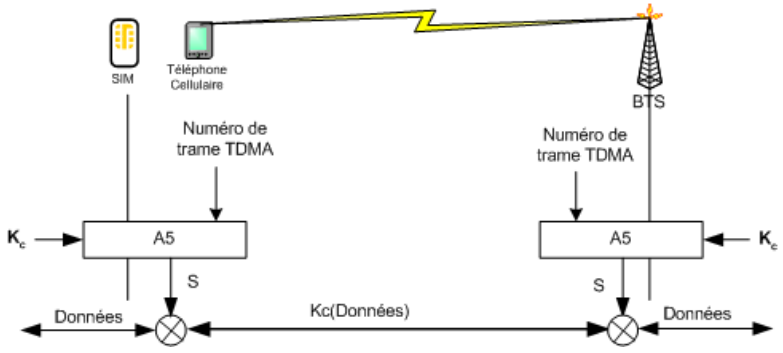


Figure 13 *Chiffrement GSM et algorithme A5*

11.3.3. Lacunes Sécuritaires dans l'accès radio GSM

Les mécanismes de sécurité mis en œuvre dans le GSM permettent d'obtenir des niveaux de protections très élevés pour le système et pour les utilisateurs. En effet, il faudrait, par exemple, plusieurs milliards de couple (RAND, SRES) afin de déterminer l'algorithme A3. Mais aucun système n'est fiable à 100%. Les failles les plus probables proviennent de situations ou le système doit transmettre certaines informations sensibles en clair. Notamment, bien que les transmissions radio soient sécurisées, il n' y a pas de chiffrement sur le NSS qui repose sur SS7. Le problème revient donc à la sécurisation de signaux de signalisations, ce qui n'est pas forcements spécifiques à GSM. Nous allons donner quelques exemples de lacunes et de leurs conséquences sur des attaques possibles.
La première lacune vient de l'identification de l'utilisateur et est illustrée par la Figure 14. Comme précédemment abordé, le système utilise un identifiant temporaire (TMSI) afin de ne jamais devoir divulguer le vrai identifiant (IMSI). Cependant, en cas de perte de TMSI, ou lorsque le VLR courant ne la reconnaît pas suite à une panne, l'IMSI est transmis en clair. Dans ce cas précis, il ne peut y avoir de chiffrement de l'IMSI grâce à l'algorithme A5 étant donné que le système ne reconnaît même pas l'utilisateur et ne va donc pas lui transmettre de séquence aléatoire (RAND).

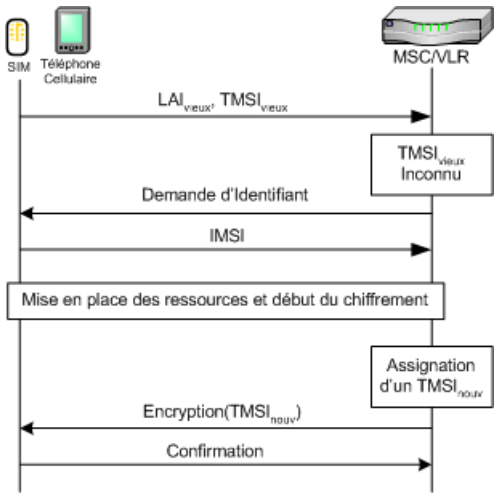


Figure 14 *TMSI inconnu et transmission de l'IMSI en clair*

Cette faille peut être exploitée en utilisant de faux relais BTS et BSC. En effet, ces relais vont donc en permanence refuser l'utilisateur jusqu'à ce qu'il transmette son IMSI. Ce type d'attaque est, en principe, peu courante dans les réseaux GSM et peut être contournée par une authentification mutuelle utilisateur et station de base. Cela n'a pas été pris en compte pour le GSM, mais a été adapté sur la sécurité de

l'UMTS. En effet, les acteurs du réseau GSM étaient considérés comme fiables alors que de nouveaux entrants dans le réseau 3G pourraient ne pas l'être.

Obtenir de manière frauduleuse une clé K_i n'est pas une mince affaire, car la clé K_i est, elle-même, chiffrée sur la carte SIM. De plus, elle ne sort jamais ni du mobile ni de l'AuC. Il y a cependant quelques failles. L'algorithme sous-jacent à A3 et A8 peut être choisi de manière indépendante par les opérateurs. Dans la pratique, le protocole COMP128 spécifié dans la norme GSM (mais jamais publié) fut utilisé. En 1998, Briceno, Goldberg, et Wagner ont rétro-conçut COMP128, puis ont effectués des analyses qui ont permis de mettre à jour une faille afin d'obtenir la clé secrète K_i [ISA 98]. Bien que cette faille fût comblée par COMP128-2, il fut démontré qu'il était théoriquement possible de cloner une carte SIM. Cela nécessitait cependant de bons équipements et un peu de temps (environ 8 heures). Plus récemment, Rao, Rohatgi, Scherzer, et Tinguely ont réussi à obtenir la clé K_i, mais cette fois, en moins d'une minute [RAO 02].
Le chiffrement original du GSM fût A5/1, qui était limité à l'utilisation en Europe. Suite au succès mondial du GSM, une version faible A5/2 fut mise au point. Similairement à COMP128, ni A5/1 ni A5/2 ne furent publiés, mais furent rétro-conçût en 1999. Suite à cela, Biryukov, Shamir, et Wagner [BIR 00] ont illustré la faiblesse de l'algorithme de chiffrement A5/1 et A5/2 en parvenant à obtenir la clé de chiffrement K_c simplement à l'aide d'un ordinateur personnel comme centre de calcul. En 2003, Barkan, Biham, et Keller [BAR 03] ont décrit une série d'attaques sur les algorithmes A5/1, A5/2, A5/3 et même GPRS, qui permettent, en théorie, d'obtenir la clé de chiffrement K_c et de déchiffrer les conversations en temps réel. Les opérateurs migrent lentement vers des versions plus sure des algorithmes de sécurité GSM. Cependant cette mise à jour reste lente étant donné qu'elle est sous-jacente au remplacement des cartes SIM des utilisateurs.

Une seconde faille est le clonage de carte SIM. Si un attaquant parvient à cloner une carte SIM et allume le mobile, le réseau va détecter qu'il y a deux mobiles avec les mêmes identifiants en même temps. Il va donc fermer la souscription, empêchant par là toute usurpation active d'identité. Cependant, cela n'est pas le cas si l'attaquant n'est intéressé que par l'écoute des communications. En effet, l'intrus a accès à la clef K_i et reçoit le RAND. Il peut donc générer la clé de session K_c et déchiffrer passivement les communications entre un mobile et la station de base où ils se trouvent. Des solutions ont été proposées afin de lutter contre cette attaque en injectant des mécanismes de contrôle de copie dans les cartes SIM.

Une manière plus simple d'écouter les conversations d'utilisateurs vient de l'utilisation de fausses bornes BTS et BSC. En effet, bien que les mobiles doivent s'identifier auprès de l'opérateur, aucune forme d'authentification n'a lieu pour l'opérateur. Il suffit donc à des intrus de s'assurer que leur station de base ait un signal plus puissant que tous les autres autour du mobile afin qu'il se verrouille sur elle. Ensuite, en désactivant le chiffrement radio, car l'intrus ne peut générer la clé

K_c, la fausse station de base peu écouter les communications transmisses de tous les téléphones mobiles passées à travers leur BTS. L'intrus peut aussi passer ou recevoir des appels qui seront facturé à l'utilisateur.

Les transmissions ne sont cryptées qu'entre la station mobile et la station de base. Si un intrus arrive à accéder à la signalisation de l'opérateur, il peut aussi écouter tout ce qui est transmis, le NSS utilisant la signalisation SS7 non sécurisée.

En conclusion, les failles majeures du GSM proviennent de l'absence d'authentifications mutuelles, de transmissions en clair, dans certains cas, de secrets qui ne devrait jamais l'être, ou de la faiblesse vis-à-vis de la cryptanalyse des algorithmes A3, A5, et A8. La communauté 3GPP en a pris conscience dans la norme pour les réseaux UMTS.

11.3.4. Lacunes Sécuritaires dans la signalisation GSM

Le GSM utilise les protocoles MAP/CAP pour la signalisation entre les éléments du réseau. Fonctionnant sur SS7, il n'y a pas de mécanisme particulier de sécurité pour ces protocoles, bien que leurs perturbations puissent être la source d'importants désagréments pour les réseaux cellulaires. Notamment, l'échange d'information entre deux HLR/VLR appartenant à deux réseaux différents peut être source d'intrusions. Nous avons pu constater, dans la section 11.2.5, que la sécurisation des couches basses de SS7 était complexe. Une sécurisation au niveau applicatif semble être plus prometteuse. Bien que la communauté 3GPP envisage un abandon progressif de la pile de protocole SS7 au profit de IP, il est à prévoir une période de transition ou des nœuds MAP basé sur SS7 communiqueront avec leurs homologues basés sur IP.
Il a donc été décidé de sécuriser les protocoles historiques au niveau applicatif avec *MAPSec* [MAP 05]. Il propose trois modes de protection. Chaque message MAPSec consiste en un en-tête MAP et un corps de message protégé. Dans tous les cas de figure, l'en-tête est envoyé en clair dans le réseau. Le mécanisme d'échange de clés est relativement lourd et est dirigée par un Key Administration Center (KAC) dans chaque réseau et est régi par les accords d'itinérance entre opérateurs. Les KAC communiquent entre eux au travers d'une interface IP et négocient les clés avec IKE. La 3GPP recommande d'utiliser l'algorithme EAS (Rijndael) pour la génération des clés de chiffrement et de contrôle d'intégrité.

L'architecture MAPSec permet un *contrôle d'intégrité* des messages, un contrôle de l'*origine d'un message*, une protection contre le *rejeu* et finalement un *chiffrement* des données.

11.3.4.1. MAPSec Protection 0
Le niveau de protection 0 n'inclut aucune forme de protection. Il est donc identique au protocole MAP d'origine.

11.3.4.2. MAPSec Protection 1
Le niveau de protection 1 inclut une authentification ainsi qu'un contrôle d'intégrité. La protection s'effectue grâce à un protocole MAP (Message Authentication Protocol) et d'une clé de session d'intégrité f7 entre deux nœuds X et Y.

11.3.4.3. MAPSec Protection 2
Le niveau de protection 2 étend le niveau de protection 1 en y ajoutant la *confidentialité* du corps de message. Cela est assuré en chiffrant le corps de message à l'aide d'une clé de session de confidentialité f6, connue de X et Y.

Les associations sécuritaires s'effectuent entre deux réseaux et restent valides pendant une durée prédéterminée. De plus, leur distribution dans les nœuds MAP est du ressort du KAC. Finalement, les nœuds MAP du réseau doivent être modifiés par une série d'opérations appelées *SecureTransport* afin de supporter l'encapsulation des composants MAP effectuée par MAPSec. La Figure 15 illustre le schéma du mécanisme de protection MAPSec.

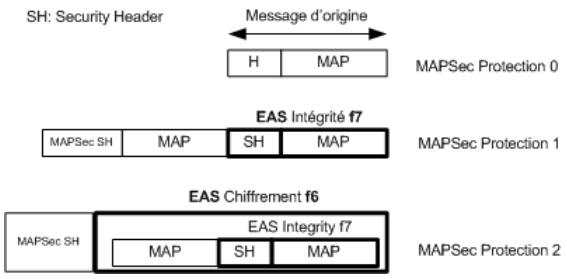


Figure 15 *Format des paquets MAPSec*

Grâce au mécanisme MAPSec, une faille significative dans la sécurisation du sous-système réseau GSM est comblée. La Figure 16 schématise l'architecture macroscopique de MAPSec.

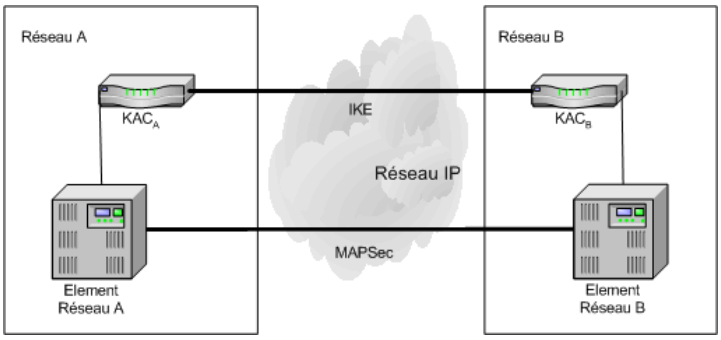


Figure 16 *Interconnexion des réseaux avec MAPSec*

11.4. Sécurité GPRS

Le General Packet Radio Service (GPRS) est une norme pour la téléphonie mobile dérivée du GSM, et permet un débit de données plus élevé pour un trafic sporadique. Il est le plus souvent qualifié de 2.5G étant à mi-chemin entre le GSM et l'UMTS. Le GPRS est une extension du GSM y ajoutant la commutation par paquet qui est plus adaptée pour la transmission de données à faible latence.

11.4.1. Architecture GPRS

Contrairement au GSM, le GPRS est capable de fournir une connectivite IP à un terminal mobile en mode paquet, et assure un débit supérieur en allouant les ressources radio en fonction du volume d'information à transférer. D'un point de vue architecturel, le réseau GPRS existe en parallèle au réseau GSM, utilisant ce dernier pour acheminer les appels voix et utilisant ses propres structures pour la transmission des données. Le GPRS ajoute donc deux nouvelles entités :

- *Serving GPRS Support Node (SGSN)* : gère les attachements des terminaux mobiles de la zone de service et réalise l'interface de transit des paquets avec la passerelle GGSN. Le lien entre le SGSN et le GGSN utilise le protocole IP mais le trafic utilisateur est encapsulé dans un protocole propriétaire appelé *GTP (GPRS Tunneling Protocol).* Concernant la sécurité, le SGSN a le même rôle que le BSC. Il gère l'authentification de l'abonné, l'intégrité des données et l'autorisation des communications.
- *Gateway GPRS Support Node (GGSN)*: est une passerelle d'interconnexion entre le réseau paquet des opérateurs mobiles et les réseaux IP. Le GGSN a la charge de gérer un pare-feu afin de contrôler d'accès au réseau de l'opérateur, il collecte les données de trafic pour la taxation, il gère les sessions ainsi que les informations de routage. Il fournit finalement une

adresse IP à un terminal mobile pendant toute la durée de la communication.

On peut identifier trois interfaces principales dans le réseau GPRS

- Gp : Interface entre deux opérateurs mobiles, mise en place principalement pour le nomadisme, au travers de routeurs de bordure.
- Gi : Interface entre un opérateur mobile et un réseau externe comme Internet ou un réseau d'entreprise au travers du GGSN
- Gn : Interface entre des GGSN et les SGSN d'un même opérateur.

La Figure 17 illustre les éléments du GPRS et leur interconnexions.

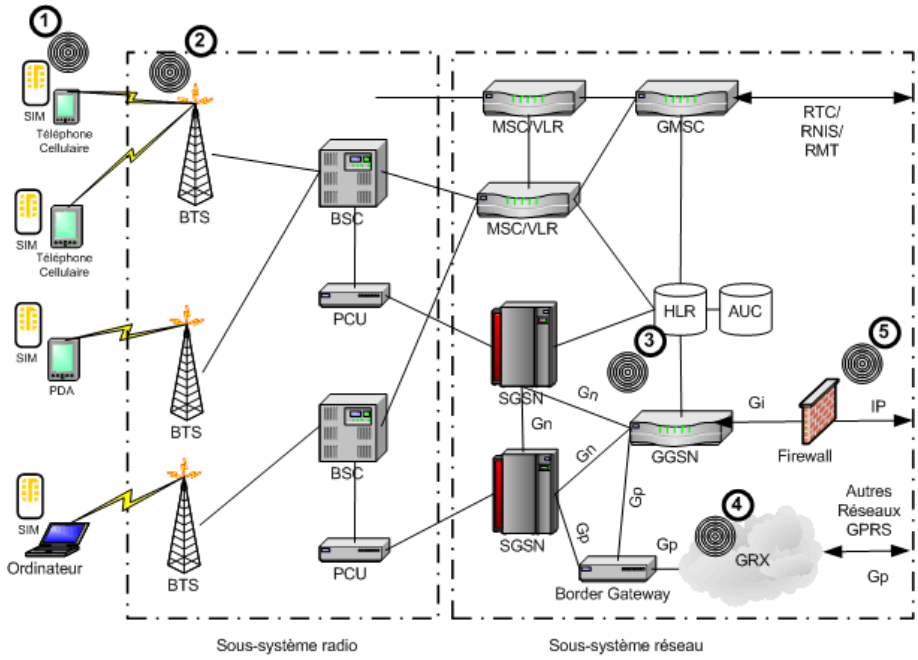


Figure 17 *Architecture du GPRS*

11.4.2. Mécanismes de Sécurité GPRS

Le GPRS ayant été aussi développé à des fin applicatives, la sécurité GPRS doit être analysée au niveau structurel et aussi au niveau des applications développés sur GPRS. La sécurité structurelle peut être décomposée en trois parties : le contrôle d'accès au réseau GPRS, le contrôle d'accès aux sessions GPRS, et le contrôle

d'accès au sous-système réseau GPRS. Nous illustrons dans la suite les divers mécanismes sécuritaires du GPRS. Nous suggérons au lecteur intéressé de se référer à la spécification 3GPP du GPRS [GPR 02,PDN 05,GEA 03] afin d'obtenir plus de détails.

11.4.2.1. Contrôle d'accès au réseau GPRS

La majeure partie des mécanismes de sécurité GPRS est identique à celui du GSM, notamment l'identification, et le contrôle d'accès. Cependant, la rupture avec le GSM provient de la sécurisation des paquets et non plus d'un appel ou d'une connexion. Cela impacte le chiffrement qui s'effectue au niveau protocolaire et non plus au niveau de la couche physique.

11.4.2.1.1. Authentification des utilisateurs GPRS

L'authentification des utilisateurs sur un réseau GPRS est similaire à celle d'un réseau GSM. En revanche, du côté du réseau, la différence majeure est que l'authentification n'est plus assurée par la station de base mais par le SGSN, et utilise un nombre aléatoire GPRS-RAND différent et indépendant du GSM. Cela a pour conséquence de produire une réponse au défit (GPRS-SRES) et une clé de chiffrement (GPRS-K_c) distinctes du GSM.

11.4.2.1.2 Chiffrement des transmissions GPRS

Le chiffrement des données et de la signalisation GPRS est basée sur le protocole GPRS A5, plus communément appelé GPRS Encryption Algorithm (GEA) afin de le différencier de son alter ego GSM. Cependant, le chiffrement GPRS diffère en plusieurs points par rapport au GSM. Premièrement, le chiffrement n'a plus lieu uniquement entre l'utilisateur et la station de base comme pour le GSM, mais s'étend jusqu'au SGSN. La clé GPRS-K_c est stockée par le SGSN indépendamment de la clé de chiffrement K_c du GSM. Ensuite, contrairement au GSM, GPRS ne chiffre plus un canal physique, mais une trame logique de la couche LLC (Logical Link Control), étant donné que le trafic GPRS est multiplexé sur la même ressource radio. Le chiffrement s'effectue donc sur une couche protocolaire supérieure. Finalement, similairement au GSM, plusieurs versions de l'algorithme GEA existent (GEA/1, GEA/2, GEA/3). L'algorithme GEA/3 est une version simplifiée de KASUMI, un protocole contenu dans l'UMTS AKA.

Le GEA est donc renforcé de nouveaux paramètres :

- *GPRS-K_c* : Clé de chiffrement spécifique à GPRS
- *$Trame^{LLC}$* : Le numéro de trame de la couche LLC.
- *Direction* : La direction de la transmission
  (entre un utilisateur et un SGSN ou inversement)

Le but des deux nouveaux paramètres est de rendre le chiffrement spécifique à la position du paquet dans la trame TDMA ainsi qu'au sens de la transmission. La Figure 18 illustre le schéma de la mise en place du chiffrement avec GEA3.

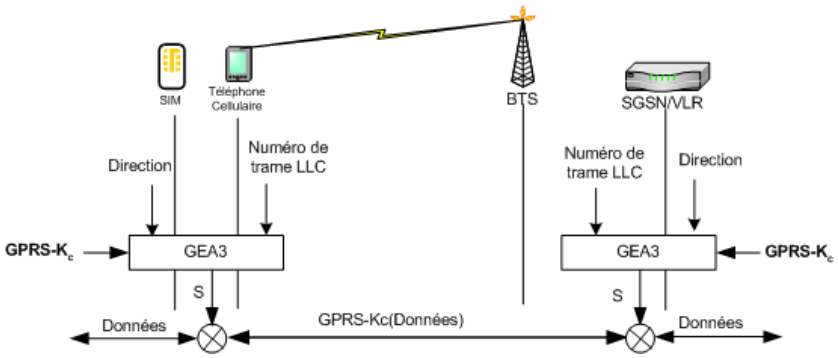


Figure 18 *Chiffrement dans le GPRS*

11.4.2.2 Le contrôle d'accès aux sessions GPRS

Contrairement au GSM, où l'accès au réseau garanti un accès aux services (SMS par exemple), le GPRS doit établir une connexion logique afin de rendre un terminal atteignable pour les services GPRS. Un mécanisme particulier a été créé, appelé *« contexte PDP » (Packet Data Protocol)*, qui permet d'établir un lien logique entre un terminal mobile, un SGSN et un GGSN et de rendre le terminale mobile visible depuis des réseaux de données (Internet, intranet, etc..). Un contexte PDP attribue donc une adresse IP au mobile et définit les contextes de routage, de sécurité, de facturation ou de qualité des services fournit par le réseau GPRS. Par allusion à Mobile IP, dans un contexte PDP, un GGSN joue le rôle de Home Agent (HA), alors que le SGSN est un Foreign Agent (FA).

Un contexte PDP peut être établis après un GPRS Attach (processus similaire, bien que plus complexe, à un enregistrement GSM). Le PDP a la charge de gérer les sessions GPRS, d'établir un tunnel logique entre un terminal mobile et un point d'accès GGSN pour les services IP, et de mettre à jours les informations de routages contenues au point d'accès GGSN lors d'itinérances.
Un contexte PDP peut être

- *Statique* : Dans ce cas, une adresse IP publique et statique est attribuée soit par l'opérateur, soit par le fournisseur d'accès Internet (FAI) lors de la souscription.

- *Dynamique* : Dans ce cas, une adresse IP publique et dynamique est attribuée lors de l'établissement du contexte PDP.

De plus, un contexte PDP permet l'établissement d'un accès à Internet transparent ou non-transparent.

- *Accès IP transparent* : Une adresse IP statique ou dynamique est établie par l'opérateur GPRS et son serveur DHCP. L'utilisateur n'a donc pas besoin de s'authentifier à nouveau lors de la création du contexte PDP. Aucune forme de sécurité ou de confidentialité n'est assurée ni sur le réseau cœur GPRS, ni sur les réseaux IP traversé. Par conséquent, suivant les services désirés par un utilisateur GPRS, une seconde authentification peut être demandée au niveau applicatif entre le fournisseur de service ou réseau privé, et l'utilisateur (p.ex IPSec VPN).
- *Accès IP non*-transparent : Une adresse IP statique ou dynamique est établie par le fournisseur d'accès Internet (FAI). Dans ce cas, l'utilisateur doit s'authentifier à nouveau auprès du GGSN lors de l'établissement du contexte PDP. Le GGSN demande l'identification de l'utilisateur et son autorisation d'accès auprès d'un serveur RADIUS maintenu par le FAI ou le réseau privé, et obtient ensuite une adresse IP par un serveur DHCP. La sécurisation des connexions entre l'opérateur GPRS et le FAI ou le réseau privé dépend d'accords mutuels.

La Figure 19 illustre un schéma d'établissement de *contexte PDP non-transparent*, suivant un *GPRS Attach*. Afin d'améliorer la clarté, seuls une parties des messages sont illustrés.

11.4.2.3 Le contrôle d'accès au réseau GPRS

Afin de gérer l'itinérance entre différents opérateurs GPRS sans devoir utiliser Internet comme intermédiaire, la norme 3GPP a créé *un GPRS Roaming Exchange (GRX)*. Il s'agit d'un réseau IP sécurisé reliant les opérateurs GPRS entre eux sur l'interface Gp et sert à acheminer du trafic en itinérance, des informations concernant l'utilisateur en itinérance ou des informations relatives à un DNS. Un GRX n'est en aucun cas connecté à Internet. A travers un GRX sont reliés directement des SGSN visités au GGSN du réseau de base de l'utilisateur en itinérance. Afin de contrôler les flux entrant dans leur réseau, les opérateurs ont inclus un *Border Gateway (BGW)* comme passerelle entre deux réseaux GPRS. Les messages sont acheminés à l'aide du protocole *GPRS Tunneling Protocol (GTP)* reposant sur IP. Il n'inclut aucune forme de sécurité et peut être donc source d'attaques.

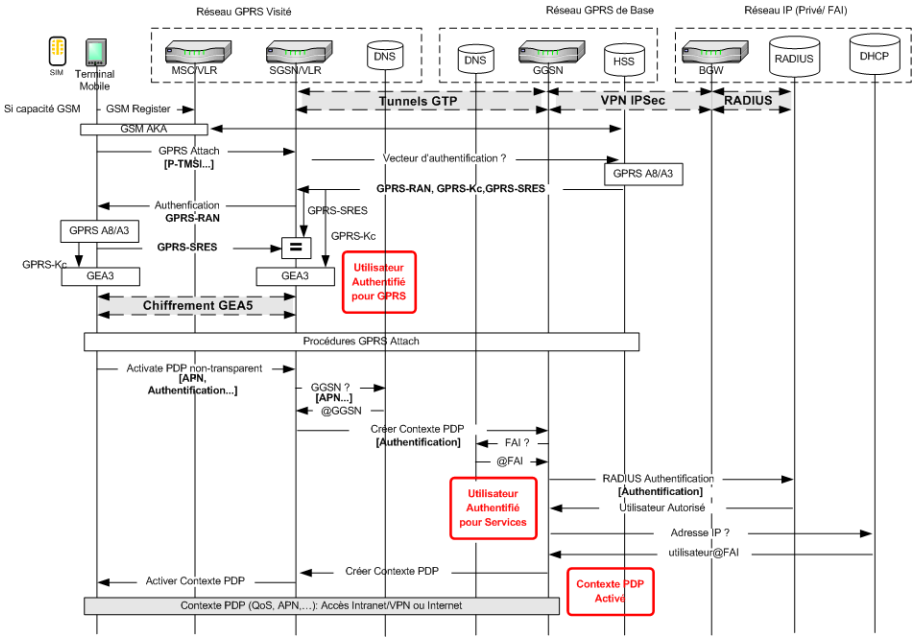


Figure 19 ***Etablissement d'un contexte PDP***

Le second point d'accès au réseau GPRS est le GGSN lui-même à travers l'interface Gi. Il s'agit du seul élément qui protège le réseau GPRS du monde Internet et filtre l'accès au réseau à l'aide d'un pare-feu.

11.4.3 Exploitation des Failles Sécuritaires du GPRS

Sur la Figure GPRS, nous avons illustré cinq points du réseau GPRS sensibles aux attaques

- sur le terminal mobile ou la carte SIM
- sur le lien radio GPRS
- sur l'infrastructure interne du GPRS (Interface Gn)
- sur l'interconnexion entres les opérateurs GPRS (Gp)
- sur l'interconnexion avec Internet (Interface Gi)

Nous résumons dans la suite divers cas d'attaques possibles sur le réseau GPRS. Pour une description plus approfondie, nous suggérons au lecteur de se référer à [XEN 06].

11.4.3.1 Attaque sur le terminal mobile ou la carte SIM

Bien qu'amélioré depuis les apparitions d'attaques de ce genre sur le GSM, cette partie n'en reste pas moins sensible à l'usurpation et à la compromission.
Les algorithmes d'authentifications de la carte SIM étant identiques à ceux du GSM, des attaques similaires à celles décrites dans la section 11.3.3. peuvent être conduites.
Un nouveau vecteur d'attaque sur le réseau GPRS provient cependant aussi des terminaux mobiles, qui interagissent avec un système informatique et, à travers GPRS, aussi à Internet. On peut dès lors imaginer l'action de virus informatiques, ou autres vers très répandu dans le monde Internet. Le téléphone cellulaire GPRS n'en est pas moins en reste, étant donné que lui aussi comporte un système d'exploitation basic qui peut être théoriquement compromis.
Un virus peut altérer un service GPRS afin qu'il émette discrètement du trafic vers certaines destinations, potentiellement illégales. Les opérateurs GPRS facturant les communications à travers leur réseau en fonction du débit, cela peut avoir des conséquences financières non négligeables.

11.4.3.2 Attaques sur le lien radio GPRS

Bien que le chiffrement GEA3 soit plus élaboré que celui du GSM, il n'en reste pas moins une cible d'interception et d'écoute. GEA3 est, certes, basé sur le protocole de chiffrement KASUMI, il n'en est qu'une version simplifiée afin de pouvoir être utilisé même avec les ressources limitées des téléphones GSM/GPRS actuels. Notamment, la longueur de la clé de chiffrement K_c n'est que de 64 bits, ce qui est absolument trop faible pour assurer une confidentialité des communications. Barkan, Biham, et Keller [BAR 03] ont d' ailleurs décrit une attaque théorique sur GEA.

11.4.3.3 Attaques sur l'infrastructure interne du GPRS (Interface Gn)

Similairement au réseau GSM, l'infrastructure du réseau cœur GPRS est très vulnérable. En effet, étant en partie basée sur le protocole SS7, elle en hérite toutes les failles. Le protocole GTP (GPRS Tunneling Protocol) basé sur IP n'étant pas sécurisé, l'écoute ou l'interception de messages échangés entre SGSN et GGSN est envisageable. Un intrus peut aussi générer des attaques de « déni de service » sur la signalisation ou tenter d'obtenir des informations du HLR, ou de l'AuC. Il est donc recommandé d'utiliser des protocoles comme MAPSec ou IPSec sur l'interface Gn.

11.4.3.4 Attaques sur l'interconnexion entres les opérateurs GPRS (Gp)

Le point critique de la sécurité structurelle GPRS est le GGSN. En effet, il est le seul élément du réseau qui protège le PLMN du monde IP, et est le seul point d'accès du réseau pour les réseaux externes. Héritant des lacunes de signalisation

interne au NSS, il n'y a pas d'authentification entre les SGSN et les GGSN. La compromission d'un GGSN peut avoir des conséquences dramatiques sur le fonctionnement du réseau.
Une exploitation de cette faille peut être mise en place en bénéficiant de GTP et de GRX. Le GTP est un protocole reposant sur IP utilisé afin de gérer le nomadisme dans les réseaux GPRS. Il n'inclut notamment aucune forme de sécurité. Il est contrôlé par le SGSN afin de créer ou annuler une session, ou étendre une session d'un utilisateur provenant d'un autre SGSN. En revanche, aucun mécanisme d'authentification de SGSN n'est appliqué, ce qui a pour conséquence d'autoriser une attaque basée sur GTP. La Figure 20 illustre une telle attaque. En compromettant un SGSN simplement en se faisant passer pour un SGSN d'un opérateur, un intrus peut envoyer des paquets GTP et compromettre les services GGSN. Par exemple, il devient possible d'intercepter des paquets GTP valides et de déconnecter des utilisateurs. Il est donc recommandé d'utiliser des protocoles sécurisés comme IPSec sur l'interface Gp.

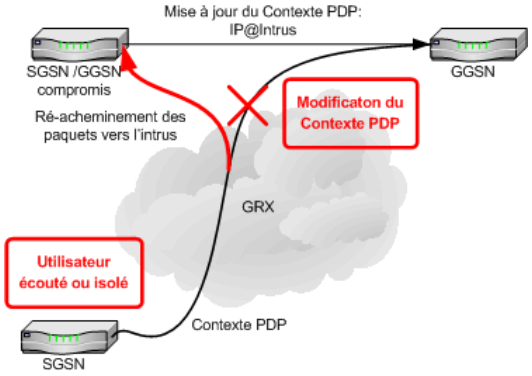


Figure 20 ***Exemple d'attaques GTP***

11.4.3.4 Attaques sur l'interconnexion avec Internet (Gi)

Les opérateurs GPRS ne sont pas seulement des cibles d'attaques depuis l'intérieur de leur réseau, mais aussi de l'extérieur. En effet, l'interface Gi interconnecte le réseau GPRS avec le réseau Internet. Cela expose donc le réseau GPRS à de multiples attaques propres au réseau Internet, comme les vers, et autres virus, dont le but principal est souvent le déni de service.
Une autre forme d'attaque potentielle est le Spam. En effet, les utilisateurs étant facturés au débit, une charge accrue des boîtes de courriers électroniques a un effet non négligeable sur la facture d'un usager.
Afin de lutter contre ce genre de menaces, les opérateurs sont protégés par un pare-feu. Cependant sa configuration reste très complexe, étant donné qu'il doit non seulement analyser le trafic IP, mais aussi incorporer les politiques de sécurité des

réseaux GPRS, comme la surveillance d'ouverture de sessions initiées à l'extérieur du réseau.

D'autres attaques sont possibles en fonction de l'interface utilisée. En revanche, elles bénéficient toutes des mêmes failles, autrement dit le manque d'authentification entre les composants d'un réseau, voire de différents réseaux, et les lacunes de GTP. De plus, on peut remarquer la forte tendance aux attaques de déni de service, très répandues dans les réseaux IP. Dans [JUN 04], Bavosa décrit les principales failles sécuritaires dans le sous-système réseau GPRS et propose des recommandations afin de les combler.
La Figure 21 résume graphiquement les différentes attaques structurelles possibles sur le réseau GPRS.

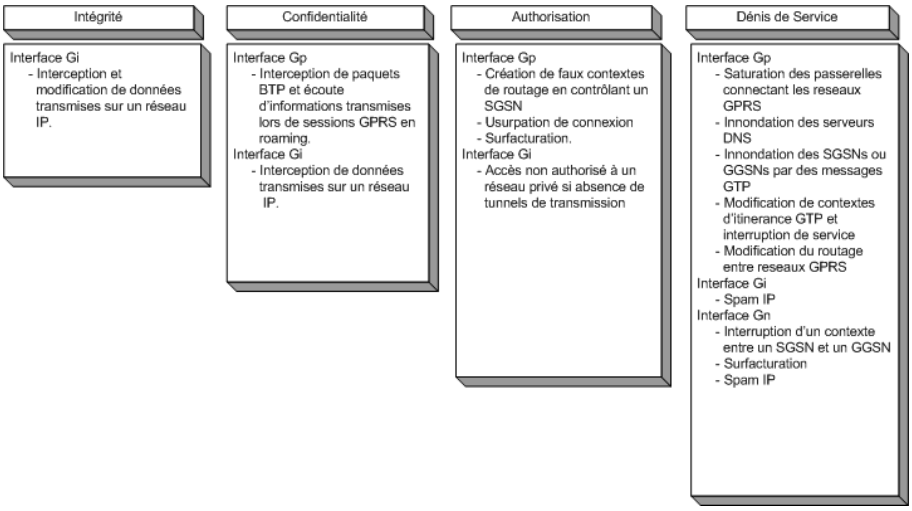


Figure 21 *Taxonomie d'attaques sur le GPRS*

11.4.4. Sécurité Applicative

Deux protocoles applicatifs furent proposés pour le GPRS, le *Wireless Application Protocol (WAP)* maintenu par le WAP forum, et l'*i-mode*, propriété de NTT DoCoMo. Nous allons décrire ici la sécurité du protocole WAP.

La technologie WAP a été créée dans le but de permettre à des terminaux mobiles d'accéder à du contenu Internet, et ce, quel que soit le type de terminal ou sa capacité d'affichage ou de traitement. Il s'agit donc de mettre en place un standard qui définisse la manière dont les terminaux mobiles accèdent à des services Internet de manière indépendante des technologies de transmissions fournies. Le WAP définit aussi la manière dont les documents doivent être structurés grâce à un langage dérivé de l'HTML appelé WML (Wireless Markup Language).
Avec l'apparition du GPRS, il est devenu possible d'obtenir des services Internet en itinérance. Cependant, deux restrictions s'imposent sur le contenu effectivement disponible à travers le WAP :

- Le réseau GPRS à une capacité limitée de transmission.
- Le terminal mobile à une capacité limitée en traitement et affichage.

Le WAP se propose donc de définir un standard décrivant des protocoles adaptés aux réseaux et aux terminaux.

La manière classique d'accès est de demander un service à partir d'un navigateur dans le terminal mobile vis-à-vis d'un serveur Web. Etant donné que les capacités d'un mobile (processeur, taille, écran, etc…) sont limitées, l'approche est de simplifier l'usage d'HTML et de passer en mode binaire sur l'interface radio. Cela sous-entend donc une interface et une passerelle situées entre l'utilisateur et le réseau Internet dont la charge est d'adapter, dans la mesure du possible, les services disponibles pour le réseau cible. Cependant, chaque réseau, ou même opérateur, a des capacités et des politiques de transmissions différentes. Cette interface doit donc se situer chez l'opérateur.
En conséquence, les services disponibles à travers WAP sont situés chez un opérateur, GPRS par exemple, qui en contrôle la qualité. En fonction de sa politique, l'accès aux services peut donc être fortement limité, comme un accès limité aux couriels, ou une restriction sur HTTP.

L'architecture WAP repose sur les quatre éléments illustrés par la Figure 22. La brique cruciale dans WAP est la passerelle WAP. En effet, elle est chargée d'effectuer la transition entre le format WAP et le format Web, ainsi que du transfert des éléments de sécurités du monde WAP et Web.

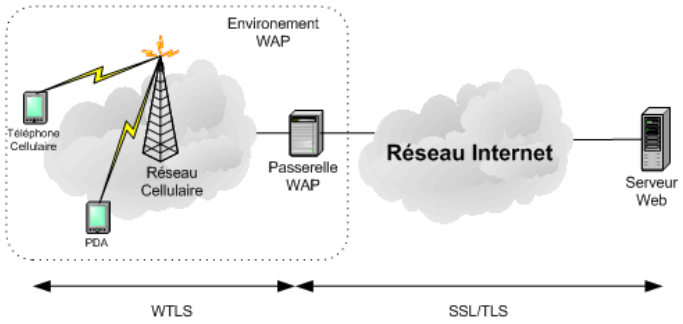


Figure 22 *Architecture WAP*

Dans le monde Internet, la sécurité applicative est effectuée grâce au protocole SSL, qui devrait être prochainement remplacé par TLS. Le monde WAP utilise aussi une forme de TLS adapté, appelée WTLS (Wireless Transport Layer Security). Il s'agit d'une version édulcorée de TLS contenant cependant tous les mécanismes sécuritaires de TLS, à savoir les échanges de clés, signatures, chiffrement symétrique et fonction de hachage. La passerelle WAP a donc la charge d'effectuer la transition entre WTLS et SSL ou TLS. WTLS a été remplacé par une spécification plus complexe de sécurité de bout en bout dans WAP 2.0.

Le WTLS fournit les mécanismes de sécurité suivants :

- *Confidentialité* : Chiffrement symétrique de type DES, 3DES, RC5, ou IDEA.
- *Authentification et échange de clés* : Certificat de type RSA, Diffie-Hellman, ou Courbes Elliptiques Diffie-Hellman.
- *Contrôle d'intégrité* : Digest HMAC de type MD5 ou SHA-1.

Bien que WTLS ait été inspiré de TLS, il comporte cependant des failles cryptographiques non négligeables, principalement par simplification d'hypothèse de TLS [WTL 01]. Par exemple :

- *Troncation des clés de Hachage* : Afin de réduire les coûts de transmission, les messages Digest HMAC servant à l'intégrité des messages peuvent être tronqués. Par exemple, le SHA-40 définit dans WTLS utilise SHA-1 afin d'obtenir un HMAC de 40 octets. Cependant, il ne considère que les 5 premiers octets.
- *Man-in-the-Middle* : La passerelle WAP chiffre et déchiffre les messages WAP. Si elle est compromise, elle peut jouer le rôle de « man-in-the-middle » tout à fait légitimement.
- *Oracle* : Certains messages d'erreur envoyés sans chiffrement permettent d'obtenir des informations sur le chiffrement d'un message.

- *Interopérabilité* : Afin que WAP puissent fonctionner sur toutes sortes d'appareils mobiles, même avec des capacités de ressources limitées, il est possible d'utiliser des méthodes sans chiffrement ou utilisant un chiffrement simplifié.

Sengodan, Smith and Abou-Rizk [SEN 00] ont illustré les différences sécuritaires entre WTLS et TLS. Saarinen a décrit dans [WAP 99] des exemples d'attaques théoriques sur le protocole WTLS.
La version 2.0 de WAP propose cependant certaines améliorations, comme un TLS bout en bout, ou des profils HTTP et TCP sur l'interface sans fils, et supprime les traitements de chiffrement / déchiffrement de la passerelle.

11.5. Securité 3G

L'Universal Mobile Telecommunications System (UMTS) est l'une des technologies de téléphonie mobile de troisième génération (3G). Le but de l'UMTS est multiple. L'UMTS présente les avantages qui s'appliquent autant aux communications vocales qu'aux transferts de données. Comme la technologie emploie une bande de fréquence plus grande, elle peut faire passer plus d'appels en même temps. De plus, son débit est augmenté de manière significative. En théorie, l'UMTS devrait remédier à la saturation des réseaux existants et proposer des services de meilleure qualité. Le débit jusqu'un cinq fois plus rapide laisse entrevoir notamment l'émergence d'applications multimédia.

11.5.1. Infrastructure UMTS

Le réseau UMTS a été contraint d'assurer une compatibilité totale avec le réseau GSM. Son infrastructure inclus donc les fonctionnalités GSM et UMTS comme illustré dans la Figure 23.

L'UMTS reprends très largement les entités GSM et GPRS pour les appels vocaux ou pour la transmission de données. La différence s'effectue au niveau protocolaire pour chaque interface ainsi qu'au niveau technologie radio. Deux nouveaux nœuds se différencient par rapport au GSM/GPRS :

- Node B : Remplace le BTS
- Radio Network Controller (RNC) : remplace le BSC.

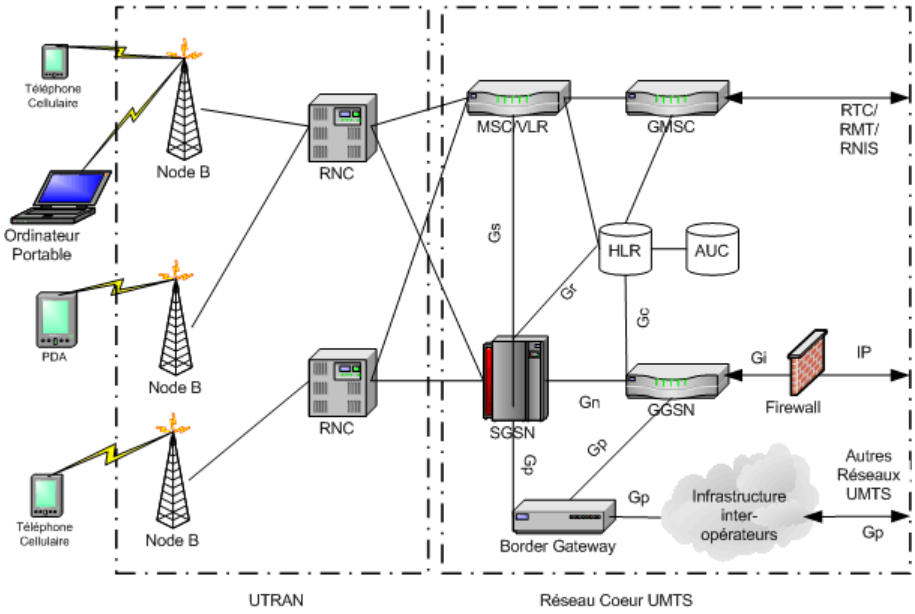


Figure 23 *Architecture UMTS*

11.5.2. Sécurité UMTS

Un certain nombre de systèmes de sécurité dits de troisième génération définissent une gestion sécuritaire accrue dans les réseaux UMTS, parmi lesquelles la détection des fausses stations de base, la limitation de la transmission de clés d'encodage, d'évaluation et d'identification entre réseaux, l'utilisation de clés plus longues, l'indentification indépendante de l'encodage, la protection de l'intégrité des donnes et la protection de l'identité du terminal. De plus, une puce plus puissante contenant un « *Universal Subscriber Identity Module* » (USIM) plus perfectionné remplace la puce SIM du GSM.

La rupture dans la téléphonie de troisième génération est principalement l'hétérogénéité des opérateurs. En effet, on assiste non seulement à une interconnexion de nouveaux opérateurs de téléphonie cellulaire, mais aussi l'interconnexion à de nouveaux types d'opérateur de télécommunications, comme les réseaux WIFI, les réseaux d'entreprises, les réseaux de téléphonies fixe, sans compter les nombreux opérateurs virtuels à tous les niveaux. Cela nécessite donc une gestion de la sécurité accrue au niveau de la signalisation et du transfert d'information du côté du NSS. Cependant, une autre rupture de l'UMTS vient aussi de la sécurisation de la partie radio du réseau. En effet, les terminaux UMTS disposant de ressources supplémentaires, il devient possible d'utiliser des

algorithmes de sécurité plus puissants comme TLS ou IPSec. De plus, une authentification mutuelle a été proposée afin de combler une lacune héritée du GSM.

La sécurité dans l'UMTS est composée de cinq catégories de protections

- *Sécurité de l'accès au réseau* : Cela inclut une authentification mutuelle entre un utilisateur et un réseau, et limite les attaques sur le sous réseau radio.
- *Sécurité du domaine réseau* : Protection de la signalisation dans le sous système réseau de l'opérateur
- *Sécurité du domaine utilisateur* : Protection de l'accès aux terminaux UMTS.
- *Sécurité Applicative* : Assure un échange sécurisé de données entre les terminaux UMTS et le réseau au niveau applicatif.
- *Visibilité et observabilité*: Assure une visibilité des mesures sécuritaires ainsi que de la dépendance de certains services vis-à-vis d'une mesure sécuritaire.

Nous illustrons graphiquement dans la Figure 24 suivante les diverses mesures sécuritaires mises en place pour l'UMTS.

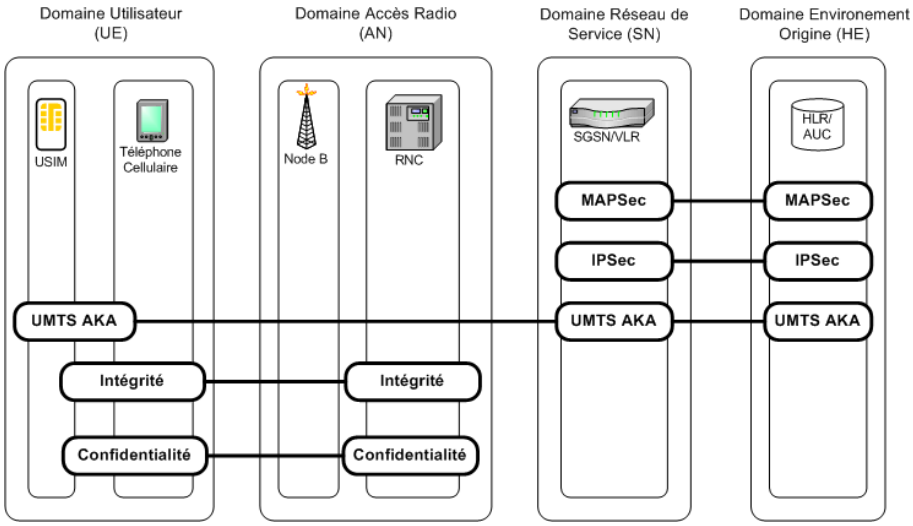


Figure 24 *Architecture Sécuritaire de l'UMTS*

La Figure 25 suivante établis la liste des algorithmes de sécurité mis en place pour l'UMTS.

Algorithmes	Signification	Status O: Opérateur S: Standard
f0	Générateur de défi aléatoire	O
f1	Fonction d'authentification de réseau	O - (MILENAGE)
f2	Fonction de génération de réponse au défi	O - (MILENAGE)
f3	Fonction de dérivation de la clé de chiffrement	O - (MILENAGE)
f4	Fonction de dérivation de la clé d'intégrité	O - (MILENAGE)
f5	Fonction génératrice de la clé d'anonymat	O - (MILENAGE)
f6	Clé de chiffrement MAP	S - (MAPSec)
f7	Clé d'intégrité MAP	S - (MAPSec)
f8	Chiffrement UMTS	S - (KASUMI)
f9	Contrôle d'intégrité UMTS	S - (KASUMI)

Figure 25 *Algorithmes de sécurité dans l'UMTS*

11.5.2.1. Accès Sécurisé au Réseau UMTS

Le nouveau mécanisme d'authentification et d'échange de clés est illustré par la Figure 26. Bien que le mécanisme sous-jacent soit similaire à celui du GSM, une différence importante est à noter. En effet, au lieu d'utiliser un triplet (RAND, SRES, K_c), le système *AKA UMTS* utilise un quintet (RAND, SRES, CK, IK, AUTN). Il est base sur le protocole MILENAGE et inclut les deux nouveaux paramètres suivants :

- *AUTN* : Un jeton d'identification du réseau. Il a été ajouté afin que l'utilisateur puisse identifier le réseau auquel il se connecte. Ce jeton est en fait constitué de trois champs
  - *Authenticated Management Field (AMF)* : Définit des opérations spécifiques à l'opérateur, comme l'utilisation d'algorithmes multiples, ou la durée de vie d'une clé.
  - *Sequence Number (SQN'=SQN* ***XOR*** *AK)* : Il s'agit du numéro de séquence définit par l'AuC de l'opérateur d'origine. Il est protégé par la clé d'anonymat AK. Il est nécessaire de protéger le numéro de séquence car il peut fournir l'identité et la position d'un utilisateur. De plus, le numéro de séquence est utilisé afin d'éviter les attaque de type rejeu.
  - *Code d'authentification de message (MAC-A)* : En le comparant à la valeur calculée par l'USIM, le terminal mobile peut attester de l'identité du réseau.
- *IK* : Clé d'intégrité. Cette clef permet d'inclure un contrôle d'intégrité dans les messages transmis autant au niveau signalisation que donnée.

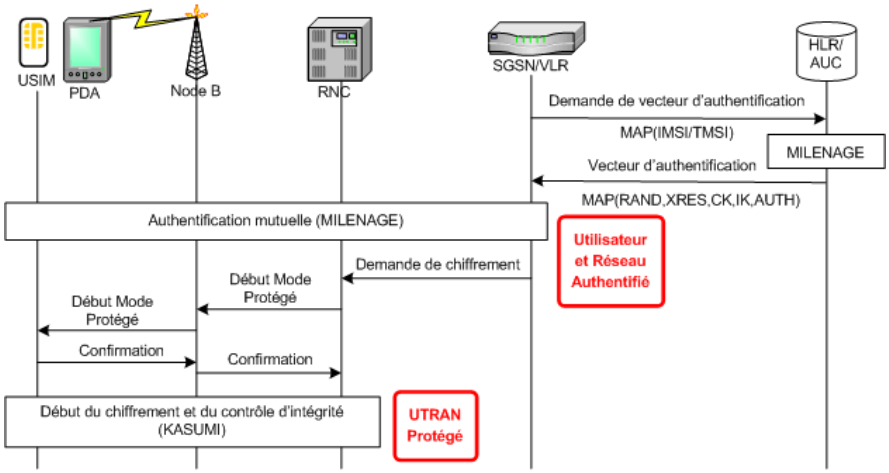


Figure 26 Schéma de l'UMTS AKA et Chiffrement

Le schéma suivant (Figure 27) est une illustration du processus d'authentification mutuelle de l'UMTS. Pour des raisons de clarté, nous n'avons pas illustré le mécanisme complexe d'obtention du champ AUTH du côté de l'AuC, ni de l'obtention du champ XMAC-A du côté de l'USIM.

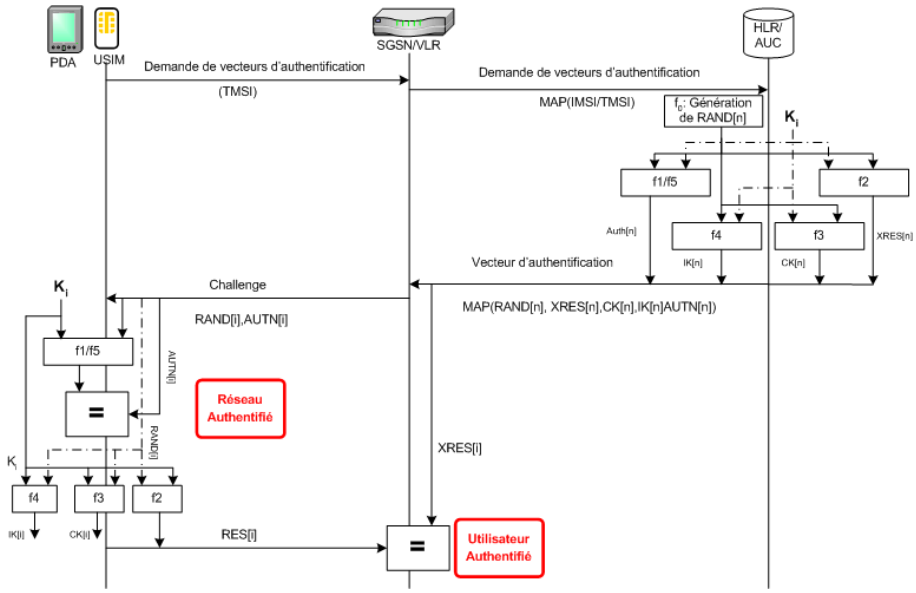


Figure 27 *UMTS AKA*

Nous avons préféré illustrer le protocole MILENAGE du coté de l'AuC et du côté de l'USIM séparément dans les Figure 28 et Figure 29.

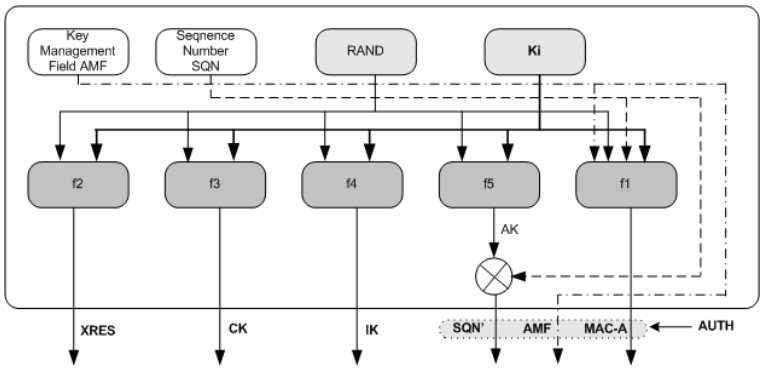


Figure 28 *Le protocole MILENAGE du côté de l'AuC*

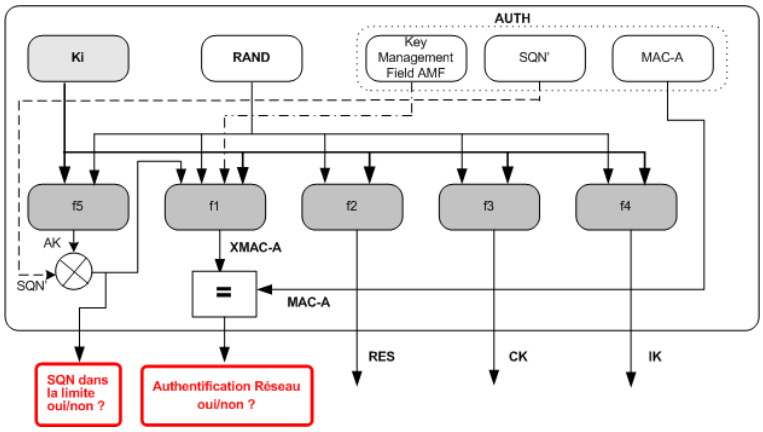


Figure 29 *Le protocole MILENAGE du côté de l'USIM*

Une autre mesure significative implémentée par l'UMTS est la gestion du chiffrement et du contrôle d'intégrité de bout en bout. Le mécanisme est basé sur le protocole KASUMI (voir Figure 30). Il consiste en un protocole de chiffrement et de contrôle d'intégrité. De plus, afin de limiter les attaques basées sur des Oracles,

certains messages de contrôle sont, au minimum, protégés contre une rupture d'intégrité, sinon déjà chiffrés. La Figure 26 illustre la procédure d'enregistrement avec demande de chiffrement.

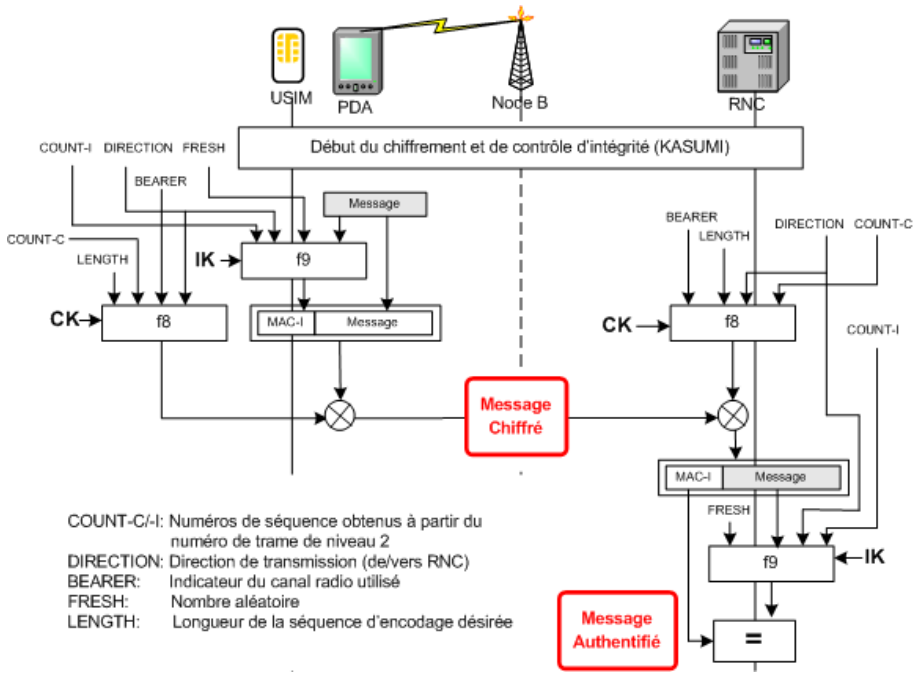


Figure 30 *Le protocole KASUMI*

En ajoutant une identification mutuelle et un chiffrement plus sécurisé incluant aussi un contrôle d'intégrité, l'UMTS AKA comble une faille majeure de l'accès au réseau du GSM/GPRS.

11.5.2.2. Sécurité d'accès au sous système réseau de l'UMTS

Le but avoué de la sécurisation du sous-système radio est de sécuriser la signalisation dans le réseau interne de l'opérateur ainsi que entre les différents opérateurs. Le système de sécurité propose de sécuriser les messages envoyés sur le réseau SS7 et aussi sur les réseaux IP. Il développe donc deux types de protocole sécuritaires : MAPSec et IPSec.

- *Mobile Application Part Security (MAPSec)* [MAP 05] : Comme abordé dans la section décrivant SS7 et GSM, la sécurisation ne peut que se faire au niveau applicatif. Nous référons le lecteur à la section 11.3.4. pour la description de MAPSec.11.3.4. 11.3.4.
- *Sécurité IP au niveau réseau (NDS/IP)* [NDS 06]: Tout protocole IP du sous système réseau utilise IPSec-ESP sans sécurisation d'entêtes. De plus, IPSec-ESP utilise le mode tunnel qui a comme but la sécurisation du message IP entre les passerelles IP. La distribution et l'échange de clés d'effectue par IKE. La Figure 31 illustre la sécurisation NDS/IP.

En fournissant deux méthodes afin de sécuriser et d'attester de l'origine des messages transmis sur SS7 et sur IP, l'UMST comble une seconde faille majeur illustrée dans les réseaux GSM et GPRS.

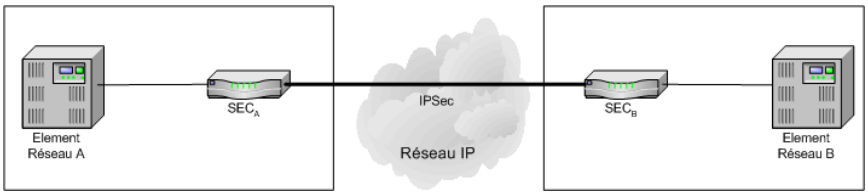


Figure 31 *Interconnexion des réseaux avec IPSec*

En conclusions, en suivant les leçons apprises du manque de sécurité des réseaux GSM et GPRS, et en profitant, non seulement des ressources plus importantes disponibles dans les terminaux mobiles UMTS, mais aussi de la puissance de la gestion et de la distribution de clés dans le monde IP, la communauté 3GPP a définit des règles de sécurités qui, si elles sont appliquées, devraient permettre de protéger les opérateurs et les utilisateurs d'intrusions non désirées.

11.6. Interconnexion des Réseaux

L'utilisation des réseaux commutés par paquets pour la transmission d'appels vocaux en temps réel en utilisant des techniques comme la Voix par paquets (VoIP), pousse à unes augmentation de la demande d'accès aux services IN de SS7. Alors que cela signifie l'interconnexion de réseaux SS7 avec Internet, cela provoque aussi l'interconnexion de réseaux SS7 avec d'autres réseaux de données. Jusqu'à présent, pour des raisons de sécurité, l'interconnexion de réseaux SS7 a été limitée. Cependant, certaines de ces raisons diminuent au regard de la demande croissante de services. En fait, les services des plateformes IN ont déjà été étendus avec succès aux réseaux cellulaires. Maintenant, des opérateurs locaux ainsi que des fournisseurs de service Internet demandent aussi un accès au réseau SS7. Des fournisseurs de téléphonie Internet voudraient proposer des services IN tels que la portabilité des numéros ou des appels gratuits sur la VoIP.

Les réseaux SS7 fournissent une très grande stabilité et résilience, mais posent des problèmes de connectivité et de sécurité. Les réseaux de données offrent une connectivité simplifiée au dépend d'une stabilité suffisante. L'interconnexion des deux pourrait être bénéfique en fournissant un accès accrus au réseau SS7 et une meilleure résilience aux réseaux de données. Cela pourrait aussi entraîner des problèmes de stabilité et de sécurité dans les réseaux SS7.

Afin de connecter le réseau Internet aux réseaux fixes, il est nécessaire de créer une interopérabilité entre SS7 et IP. A ce titre, des groupes de travail ont émergé et ont proposé quatre standards majeurs : *H.323, SIP, MGCP* et *Megaco*. Nous donnons dans la suite un bref résumé de ces protocoles, et nous référons le lecteur au chapitre relatif à la sécurité dans les réseaux mobiles de nouvelle génération pour plus de détails.

11.6.1. H.323

H.323 est un standard développé par l'IUT et définit le protocole de communication multimédia à travers des réseaux commutés par paquets.

11.6.2. SIP

Le protocole d'initiation de sessions (SIP) est un autre standard développé par IETF. SIP est un protocole de signalisation gérant principalement les appels en vidéo conférence mais aussi la téléphonie ou la messagerie instantanée lorsqu'au moins un participant appartient à un réseau commuté par paquets.

11.6.3. Megaco

Le protocole Megaco, autrement appelé H.248, fourni un contrôle et une gestion externe des communications à travers des *Media Gateway (MG)* et est complémentaire de H.323 et SIP. Les Media Gateway Controller (MGC) dirigent les MG grâce à H.248, alors qu'ils communiquent entre eux grâce a SIP et H.323.

11.7 Conclusion

La perte du monopole des opérateurs de télécommunications, ainsi que l'interconnections de différents type de réseaux (fixes, mobiles, IP) ont provoqué l'effondrement de la structure sécuritaire basée sur la réputation mise en place par les différents acteurs des réseaux de télécommunications. De nouvelles solutions ont donc été créées afin d'assurer la sécurité des infrastructures, la confidentialité des informations des utilisateur ainsi que le contrôle du contenu transmis.
Plusieurs étapes ont été nécessaires à cette fin. Premièrement, en développant les réseaux cellulaires, il a fallut sécuriser le lien radio entre le réseau et les utilisateurs. De nombreux algorithmes furent développés afin d'assurer l'intégrité, l'authentification et la confidentialité des utilisateurs. En revanche, aucune forme d'authentification ne fut jugée nécessaire envers le réseau lui-même. Ensuite, vinrent les préoccupations face aux failles sécuritaires provenant de la signalisation et de l'interconnexion de différents réseaux SS7. Cela donna naissance à de multiples rustines, mais qui n'eurent comme effet que de retarder l'abandon de SS7. L'apparition du monde IP dans les réseaux mobiles de télécommunications a permis d'utiliser des protocoles de sécurité puissants comme IPSec, et a accéléré l'apparition de nouveaux protocoles de signalisation comme SIP qui vont, à terme, remplacer SS7.
Cependant, l'interconnexion des différents réseaux ne fut qu'une autre étape vers une vision plus globale des futurs réseaux mobiles de télécommunications. Avec l'apparition d'opérateurs alternatifs ou virtuels vint la notion de service et d'interconnexion de service entre réseaux et fournisseurs. A travers cela, des nouvelles contraintes de sécurité ont vu le jour qui ont eu comme conséquence de sécuriser les services de bout en bout, et non plus à chaque segment parcouru par le service. Les réseaux mobiles de communications perdent donc de leur influence par rapport aux services eux-mêmes transmis sur leurs structures.
La nécessite de transparence ou de non transparence de l'accès au service et de son acheminement à travers une interconnexion de réseaux est un sujet à débat très actuel. L'issue est incertaine à ce stade, bien que la tendance actuelle aille vers la transparence totale. Il est fort à envisager que dans ce débat de vision et de structure des réseaux mobiles de télécommunications, l'utilisateur aura probablement le dernier mot, et qu'on assiste au retour de la sécurisation par réputation.

.

11.8. Bibliographie

[TEL 01] Telcordia, “General Function of Messages and Signals”, *Technical* Report GR-82-CORE., 2001.

[TEK 01] “Tekelec Eagle STP”, White Paper, http://www.tekelec.com/productportofolio/eagle5sas/, 2001.

[VER 02] Verizon, “SS7 Security Gatekeeper”, Technical Report Request for Information – Verizon Communications, May 2002.

[LOR 01] G. Lorenz et. al, “Securing SS7 Telecommunications Networks”, *Proceedings 2nd IEEE Workshop on Information Assurance and Security*, pp. 273-278, June 2001.

[SEN 05] H. Sengar, D. Wijesekara, S. Jajodia, “MTPSec: Customizable Secure MTP Tunnels in the SS7 Network”, *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, April 2005.

[SEI 98] Reiner Seiler, “Security Service in an Open Service Environment”, *Proceedings of the 14th IEEE Computer Security Applications Conference (ACSAC)*, pp. 223-234, December 1998.

[GSM 01] J. Eberspaecher, H.J. Voegel, C. Bettstetter, “GSM: Switching, Services and Protocols”, John Wiley & Sons, Second Edition, 2001.

[ISA 98] M. Briceno, I. Goldberg, D. Wagner, Internet Security, Applications, Authentication and Cryptography *(ISAAC)*, University of California, Berkley, see http://www.issac.cs.berkley.edu/issac/gsm-faq.html

[RAO 02] J. R. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely, “Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards”, in *Proceedings of the IEEE Symposium on Security and Privacy*, May 2002.

[BIR 00] A. Biryukov, A. Shamir, and D. Wagner, “Real Time Cryptanalysis of A5/1 on a PC”, *Lecture Notes in Computer Science*, vol. 1978, pp. 1-18, 2001.

[BAR 03] E. Barkan, E. Biham, N. Keller, ”Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication”, *Advances in Cryptology*, Vol. 2729, pp. 600-616, 2003.

[GPR 02] “General Packet Radio Service (GPRS) Service Description”, 3GPP TS 101.344, version 7.9.0, 2002.

[PDN 05] “Interworking between the Public Land Mobile Network (PLMN) supporting GPRS and Packet Data Networks (PDN) ”, 3GPP TS 101.348, version 7.10.1, 2005.

[GEA 03] “Specification of the A5/3 Encryption Algorithm for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS”, 3GPP TS 55.216, version 6.2.0, 2003.

[XEN 06] C. Xenakis, “Malicious Actions Against the GPRS Technology”, in *Journal in Computer Virology*, Springer Paris, Vol. 2, N. 2, pp. 121-133, 2006.

[JUN 04] A. Bavosa, “GPRS Security Threats and Solution Recommendations”, White Paper, Juniper Networks, 2001.

[WTL 01] “Wireless Transport Layer Security”, WAPForum WAP-261-WTLS, version 6.0, 2001.

[WAP 99] M-J Saarinen, “Attacks Against the WAP WTLS Protocol”, *IFIP Conference Proceedings*, Vol.152, pp. 209-215, 1999.

[SEN 00] S. Sengodan, D. Smith, and M. Abou-Ritzk, “On End-to-End Security for Bluetooth/WAP and TCP/IP Networks”, *in Proceedings of the IEEE Conference on Personal Wireless Communication (ICPWC’2000)*, pp. 399-403, 2000.

[UMT 05] “UMTS Security Architecture”, 3GPP TS 33.102, version 7.0.0, 2005.

[MAP 05] “MAP Application Layer Security”, 3GPP TS 33.200, version 6.1.0, 2005.

[NDS 06] “IP Layer Security”, 3GPP TS 33.210, version 7.1.0, 2006.

[KOE 02] G. M. Køien, “An Introduction to Access Security in UMTS”, *IEEE Wireless Communications*, Vol. 11, Issue 1, pp. 8-18, 2004.

[BOM 02] K. Boman, G. Horn, P. Howard, and V. Niemi, “UMTS Security”, in *IEE Journal on Electronics and Communication Engineering*, Vol. 14, Issue 5, pp. 191-204, 2002.

11.9. Index