Chapitre 12

La Sécurité dans les Réseaux Mobiles de Nouvelle Génération

12.1. Introduction

Le concept de réseaux mobiles de nouvelle génération est apparu avec l'interconnexion des réseaux de télécommunications. Au stade actuel, on assiste à une interconnexion des différentes technologies de télécommunication, avec des opérateurs proposant des services particuliers aux utilisateurs. Cependant, au delà même des différentes technologies employées, il y a aussi pratiquement un type de réseau par type de service. Par exemple, un téléphone cellulaire doté d'un accès à Internet est capable d'accéder à des services Internet limités par l'offre de service des opérateurs cellulaires. L'objectif est donc de disposer d'un réseau unique pour l'ensemble des services de télécommunication. Cependant, avec une hétérogénéité des technologies et des services, des préoccupations sécuritaires refont surface. En effet, comment assurer l'intégrité des données ou d'un réseau, ou comment assurer le contrôle de facturation des services désirés lorsqu'on a potentiellement à faire à de multiples intermédiaires ?
Dans le chapitre consacré à la sécurité des réseaux mobiles de télécommunication, nous avons abordé l'interconnexion des réseaux. Dans ce chapitre, il s'agit de mettre un pas en avant et d'envisager la convergence des services, notamment les services multimédia. Il s'agit donc d'évoluer du stade où un opérateur proposait un accès à travers des passerelles à un service situé sur une autre plateforme - ou même par un autre opérateur. L'opérateur possède, voire est, le service multimédia, et son accès est transparent pour l'utilisateur quelque soit son emplacement ou les technologies employées afin d'obtenir le service. Il devient donc concevable d'envisager

---

Chapitre rédigé par Jérôme Härri et Chrisitian Bonnet.

l'apparition du multimédia sur les téléphones mobiles, voire même d'entrevoir la transformation des opérateurs mobiles en des fournisseurs de services télévisuelles et multimédia venant concurrencer les opérateurs télévisuels publiques et privés.
Etendant la notion de session téléphonique à celle de session multimédia, le protocole SIP (Session Initiation Protocol) fut crée. Il a permis, en premier lieux, d'établir des sessions multimédia sur les réseaux Internet, mais peut aussi être employé par tout réseau basé sur un réseau Internet ou y ayant accès. Il a un fonctionnement similaire à SS7 pour l'établissement des appels, et vise principalement à le remplacer à moyen terme. L'application la plus connue de SIP est la voix par paquets (VoIP). En revanche, SIP n'est pas capable de gérer la mobilité des utilisateurs ou des réseaux. La communauté a donc proposé une extension, appelée IMS (IP Multimedia Subsystem), qui améliore le contrôle d'accès et le suivit des utilisateurs. IMS gère un accès contrôlé des utilisateurs aux réseaux ainsi que l'interconnections des réseaux. L'objectif d'IMS est d'assurer, d'une part, un accès transparent des utilisateurs aux services, d'autres part, de faciliter l'établissement de nouveaux services par des opérateurs, et ce, quelques soient les technologies employées ou l'emplacement des utilisateurs.

La voix par paquets (VoIP) fut probablement le premier service grand public bénéficiant de l'interconnexion des opérateurs de téléphonies et Internet. En effet, avec VoIP, il est devenu possible de communiquer avec un correspondant à un prix dérisoire quel que soit son emplacement, voire même gratuitement si on dispose d'un ordinateur. A travers VoIP, nous avons donc assisté au retour des services de téléphonie classique, cependant offert à travers le réseau Internet, alors que ce dernier fut historiquement conçu pour fonctionner à travers les réseaux de téléphonies classiques. De plus, avec VoIP, nous assistons aussi a l'émergence d'opérateurs virtuels de téléphonie dont nous avons très peu de contrôle, ou pour être plus précis, dont le contrôle et la sécurité ne peuvent excéder ceux proposés par Internet. En se passant complètement de l'opérateur local, l'utilisateur délègue la sécurisation de sa transmission et de ses données à un opérateur de téléphonie virtuelle dont il est parfois difficile de connaître les garanties de confidentialités. L'utilisateur accède donc à un service qui n'est contrôlé ni par l'opérateur, ni par le réseaux, laissant entrevoir des préoccupations de confidentialité, de sécurités, ou de contrôle de contenu.

Une évolution récente des réseaux mobiles est venue des applications multimédia et a généré une nouvelle vision des réseaux de télécommunications illustrée sur la Figure 1. Le nœud central étant une nébuleuse Internet sur laquelle se connectent toutes sortes d'autres réseaux (fixe, mobile, entreprise, etc..). Bien que sur le diagramme, le réseau fixe semble séparé de la nébuleuse Internet, il y a en réalité une collaboration, les opérateurs de réseaux fixes louant des lignes Internet pour leurs services, et en d'autres endroits, les opérateurs Internet louant les réseaux fixes pour leurs applications.

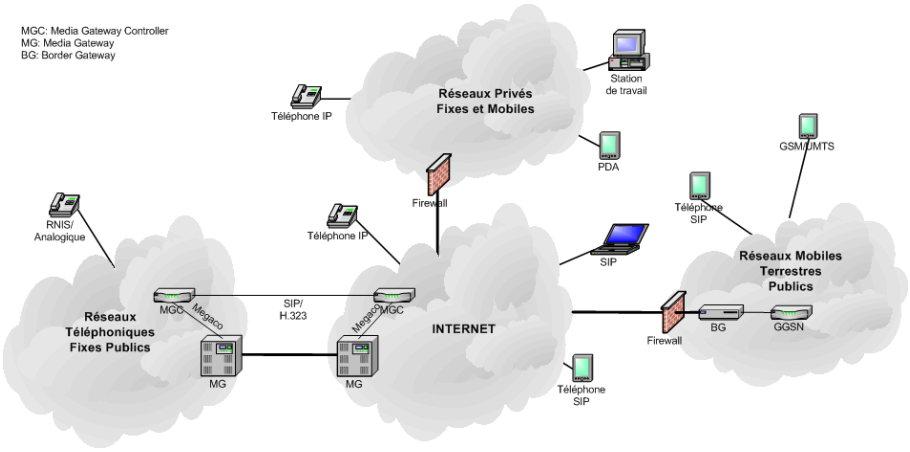


Figure 1 *Interconnexion des réseaux de télécommunication*

Avec l'interconnexion de multiples réseaux et d'opérateurs virtuels, il est important maintenant de comprendre que la sécurité des réseaux de télécommunications mobiles n'est plus spécifique aux seuls réseaux cellulaires mais doit être envisagée de bout en bout au niveau applicatif, et en collaboration avec tous les acteurs des réseaux de télécommunications, qu'ils soit fixes, mobiles ou Internet. La mobilité, ou le nomadismes des utilisateurs, ajoute d'autant plus de raisons de collaborer dans une sécurité bout en bout. Par exemple, prenons le cas de la sécurité entre un réseau opérateur et un réseau entreprise. Si la sécurité est assurée de bout en bout, l'accès au réseau Internet garanti l'accès au réseau de l'entreprise. Dans le cas contraire, nous devons d'abord nous identifier pour l'accès Internet, puis utiliser un VPN afin d'accéder au réseau entreprise. Si maintenant, on ajoute le facteur mobile de l'utilisateur, la gestion du contrôle d'accès et de la sécurité devient très difficile si elle n'est pas envisagée de bout en bout.

Dans ce chapitre, nous allons décrire les divers mécanismes de sécurité employés par les divers protocoles de signalisation et de transmissions engagés dans les réseaux de télécommunications de nouvelle génération. Notre objective est aussi de mettre en avant les failles sécuritaires ainsi que leurs exploitations possibles à des fins illicites. Avec le renforcement des mesures de sécurité, nous allons aussi aborder la gestion de la confidentialité ainsi que l'interception légale mise en place par tous les acteurs des réseaux de nouvelle génération.

12.2. Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) est un protocole d'initiation de sessions applicatives normalisé et standardisé par l'IETF. Il est chargé d'authentifier et de localiser les divers acteurs d'une communication. SIP étant indépendant du type de trafic de donnée, tout type de protocole peut donc être utilisé. Cependant, le protocole Real-time Transfer Protocol (RTP) est le plus souvent utilisé pour les sessions audio et vidéo. SIP est aussi le standard ouvert utilisé par VoIP.

12.2.1 Généralités SIP

SIP est un protocole textuel et partage des codes de réponse très similaires à HTTP. En revanche, SIP diffère de HTTP par le fait qu'un agent SIP joue à la fois le rôle de client et de server. La Figure 2 schématise le fonctionnement basic de SIP. En règle générale, SIP repose sur les éléments suivants :

- *User Agent* : On le retrouve dans les téléphones SIP ou toute application basée sur SIP. On peut établir une communication entre deux agents SIP moyennant une URI (Uniform Resource Identifier), qui est similaire à une adresse de courrier électronique.
- *Registar* : Etant donné qu'établir une communication entre deux agents SIP requière la connaissance de l'adresse IP du destinataire, le Registar est chargé d'enregistrer l'adresse IP d'un utilisateur SIP dans une base de données. Dans la base de données, l'adresse IP est liée à l'URI.
- *Proxy* : Un Proxy SIP sert d'intermédiaire entre deux agents SIP afin d'obtenir leur adresses IP respectives. Le Proxy SIP va chercher l'adresse IP de destination dans la base de données et contacte le destinataire. Le trafic de donnée ne passe pas par le Proxy mais s'échange entre deux agents SIP directement.
- *Contrôleur de Session* : Il s'agit d'un pare-feux intelligent conforme à SIP. En effectuant un appel SIP, un utilisateur met en place deux connexions, une de signalisation et une de donnée. Bien que cela ne pose pas de problème si les deux acteurs sont sur le même sous-réseau, des pare-feux ou NAT séparants les différents réseaux ne peuvent être conscient du lien entre ces deux connexions. En conséquence, un pare-feu peut rejeter un trafic de voix à destination d'un utilisateur dans son sous-réseau, même si la signalisation a été effectuée avec succès. Les NAT génèrent en plus un problème de correspondance entre des adresses multiples temporaires établies par des fournisseurs d'accès Internet, ainsi que leur visibilité dans le réseau Internet. Afin de régler ce problème, il a été proposé la création de

contrôleurs de sessions jouant le rôle de passerelle applicative assurant la correspondance correcte des adresses.

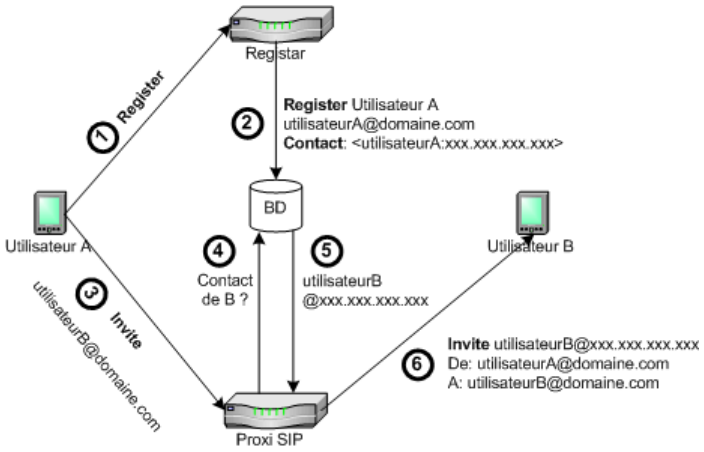


Figure 2 *Schéma de fonctionnement de SIP*

12.2.2 Failles Sécuritaires SIP

Tout comme SS7, SIP n'a pas été conçu pour contenir des mécanismes sécuritaires par défaut. Etant de plus un protocole textuel, il est très sensible aux attaques. Nous donnons quelques exemples d'attaques typiques dont des applications basées sur SIP peuvent être victimes. Pour plus de détails, le lecteur peut se référer à la spécification IETF [SIP 02] ou [SSC 03].

- *Détournement d'enregistrement* : Un Registar évalue l'identité d'un agent SIP. Le champs «From» de l'entête d'un message SIP peut être arbitrairement modifié, ce qui ouvre la porte à des enregistrements frauduleux. Cela permet donc, par exemple, à un intrus qui aurait impersonnalisé un agent SIP, de demander de retirer les adresses de contact pour un URI particulier et enregistrer les siennes à la place. Cela démontre la nécessité d'authentification entre des Agents et des Proxy SIP
- *Impersonnalisation d'un Proxy* : Un Agent SIP contacte un Proxy afin d'acheminer les requêtes. Le Proxy peut être impersonnalisé par un intrus et perturber les communications, voire rediriger les communications vers des tiers parties. La mobilité dans les réseaux augmente d'autant plus cette vulnérabilité. Lutter contre ce type d'attaque nécessite aussi la mise en place d'une authentification mutuelle.

- *Fermeture de sessions* : En écoutant passivement les paramètres d'un appel, puis en insérant un message de control SIP « BYE », un intrus peut clore prématurément une session SIP. En insérant un message « ré-INVITE », il peut aussi rediriger un appel vers une tiers partie. Afin de lutter contre cette forme d'attaque, les paramètres de connexion SIP ne doivent pas être observables et l'identité de l'agent envoyant un message de contrôle SIP doit être vérifiée.
- *Intégrité* : Il est aussi possible de modifier le contenu des messages SIP au bon vouloir des intrus. On peut aussi ne pas désirer qu'un Proxy, même authentifié, ait accès au contenu d'un message SIP, notamment lors d'échanges de clés de session.
- *Déni de Service* : Le déni de service est une forme d'attaque qui vise à rendre un élément réseau non disponible. Les Proxy SIP doivent être intégrés au réseau Internet afin d'accepter les requêtes valides en provenance d'agent SIP distribués dans le monde. Cela rend donc les réseaux SIP vulnérables à de nombreuses techniques d'attaque de type « déni de service ». A noter que si les Proxy tombent, tout le réseau SIP devient inopérationnel étant donné que les agents SIP sont incapables de se reconnaître et ne peuvent pas avoir accès à la base de donnée SIP. Une forme de lutte contre ce genre d'attaque peut être produite en contrôlant les tentatives d'enregistrement.

12.2.3. Sécuriser SIP

Une des vulnérabilités que SIP doit et peut combler assez rapidement est l'intégrité de ses messages de signalisation. Une des solutions est « *Secure SIP* » qui a recourt à des canaux chiffrés créés par le protocole *Transport Layer Security (TLS)*. Utilisé initialement afin de sécuriser les sessions HTTP, TLS peut être reconfiguré afin de sécuriser les sessions SIP contre l'écoute (eavesdropping) ou la modification de données (tampering).

L'authentification basée sur l'algorithme HTTP Digest (MD5) permet de s'assurer de l'identité d'un Agent et d'un Proxy SIP. Ce protocole est basé sur la combinaison de défis et de qualifications. Afin de limiter la transmission d'informations confidentielles entre les Registars et les Agents SIP, l'échange de certificats s'effectue à travers un canal TLS, évitant ainsi aussi des attaques de rejeux par interception de qualifications.

Les Proxy SIP s'authentifient auprès d'agents SIP locaux ou auprès d'autres Proxy grâce à des certificats TLS vérifiables globalement, puis délèguent la confiance aux Proxy intermédiaires lors de l'établissement des communications. Par exemple, un Proxy SIP ne peut pas savoir comment un Agent SIP a été authentifié par un autre Proxy SIP situé dans un autre domaine, mais puisqu'ils ont établis un canal TLS entre eux, il lui fait confiance.

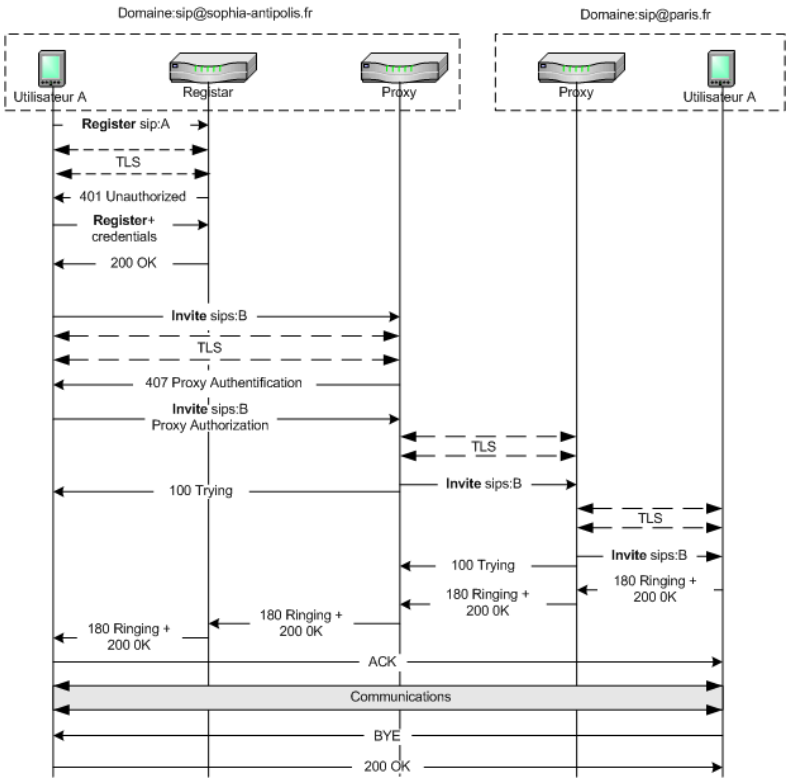


Figure 3 *Communications SIP avec sécurisation des messages*

Un autre critère de confiance assuré par SIP provient de l'emploi d'adresse SIP sécurisées SIPS. Similairement à HTTPS, lorsqu'un agent tente de contacter un autre agent SIP en utilisant une adresse sécurisée, une connexion TLS est établis sauts par sauts entre l'agent SIP et le Proxy situé dans le domaine du destinataire. En revanche, les associations sécuritaires entre ce Proxy et le destinataire reste du ressort de la politique sécuritaire du domaine visé.

L'utilisation d'IPSec AH ou ESP afin d'assurer l'intégrité ou la confidentialité des messages SIP de bout en bout n'est pas possible, les Proxy SIP ayant besoin d'avoir accès en lecture et même en écriture aux en-têtes SIP afin assurer un acheminement correcte des messages. Il est cependant possible d'utiliser IPSec AH ou ESP saut à saut. L'avantage principal de l'utilisation d'IPSec par rapport à TLS est qu'il

supporte des transmissions TCP et UDP. Finalement, une autre solution est d'utiliser S/MIME. En effet, SIP pouvant transporter des messages MIME, S/MIME permet aux Agents SIP de protéger le contenu des messages SIP sans affecter les en-têtes. L'emploi de S/MIME afin de sécuriser les communications de bout en bout à l'aide de tunnels SIP est également possible. Afin de ne pas éliminer des paquets légitimes dont les en-têtes auraient été modifiées, la RFC SIP suggère une série de règles qui permettraient de différencier les messages légitimes des attaques.
La Figure 3 illustre un exemple d'échange de messages lors d'un enregistrement puis un établissement de communication entre deux agents SIP en incluant les mécanismes de sécurité décrits précédemment.

Finalement, une dernière remarque concernant la sécurisation de SIP provient de la visibilité des utilisateurs. En effet, afin de pouvoir recevoir des appels SIP, il faut rendre visibles au réseau Internet deux adresses IP publiques - une pour la signalisation et une pour les données. Cela revient donc à diffuser sur Internet votre adresse et laisser la porte ouverte. Etant une source de préoccupation majeure de la part des fournisseurs d'accès Internet, ils établissent donc des contrôleurs de sessions situés à l'extérieur du pare-feu et qui jouent en fait le rôle de boîte postale.

12.3. Voix par paquets (VoIP)

La voix par paquets (VoIP) est une nouvelle technologie qui a permis de fédérer les mondes des communications de données et celles de la voix. En effet, avant VoIP, la seule solution pour transmettre des communications vocales était d'établir un lien circuit entre un appelant et un appelé. Ce genre de communication avait l'avantage d'être de très bonnes qualité, au dépend d'un prix tout aussi élevé. A l'heure des communications Internet, cela devenait absurde de pouvoir transférer des millions de bits de données à travers le monde à un prix très faible, mais devoir payer le prix fort pour pouvoir parler. VoIP permit donc de transmettre de la voix en temps réel à travers des réseaux principalement Internet jusqu'à présent, mais qui pourront se généraliser avec les NGN à tous les acteurs de communications.
La VoIP dépend d'une couche de signalisation et d'une couche de transport. Le protocole de signalisation, principalement H.323 du coté des opérateur mais SIP semble prendre l'ascendant depuis peu, s'occupe de localiser un utilisateur, et de débuter ou d'interrompre une communication. La couche de transport de media utilisée est principalement le RTP (Real-time Transport Protocol) et assure la partie voix de la communication en digitalisant et en encodant les communications. Finalement, IP encapsule les paquets VoIP afin d'assurer un acheminement à travers le réseau.
VoIP a été pensé pour être inter-opérable. En effet, si des appels ont lieux dans un même réseau sans fil, ou un même réseau IP, il n'a pas besoin d'autre structure. Cependant, si des appels sont émis de ou à destination de réseaux à commutation de circuits (RTC ou RMT), alors VoIP requière de nouveaux éléments :

- *Media Gateway (MG)* : Un media Gateway interrompt une communication vocale d'un réseau à commutation de circuits, échantillonne la voix et la délivre aux réseaux IP. Il effectue l'opération inverse lors d'appels à partir de réseaux IP.
- *Media Gateway Controller (MGC)* : Autrement appelé "soft switch", son rôle est d'assurer l'attribution des ressources aux MG.
- *Signaling Gateway (SG)*: Il fournit une interconnexion transparente entre le réseau de signalisation SS7 des opérateurs de réseaux commutés par circuits et le réseau IP. Il a comme rôle d'interrompre la signalisation SS7 si nécessaire, ou de la traduire au format IP et de l'acheminer aux MGC. Etant donné que ces passerelles sont vitales pour un réseau VoIP, ils sont couramment déployés par essaims.
- *IP-enabled Service Control Point (IP-SCP)* : Il a les mêmes tâches qu'un SCP ordinaire mais il est complètement intégré au réseau IP. Il est de plus complètement accessible par SS7.

Ces éléments ne sont cependant pas uniques et dépendent des groupes de recherche. Par exemple, pour H.323, MGC est appelé un « Gatekeeper (GK) », alors que les SG les MG sont simplement appelé « Gateway ».

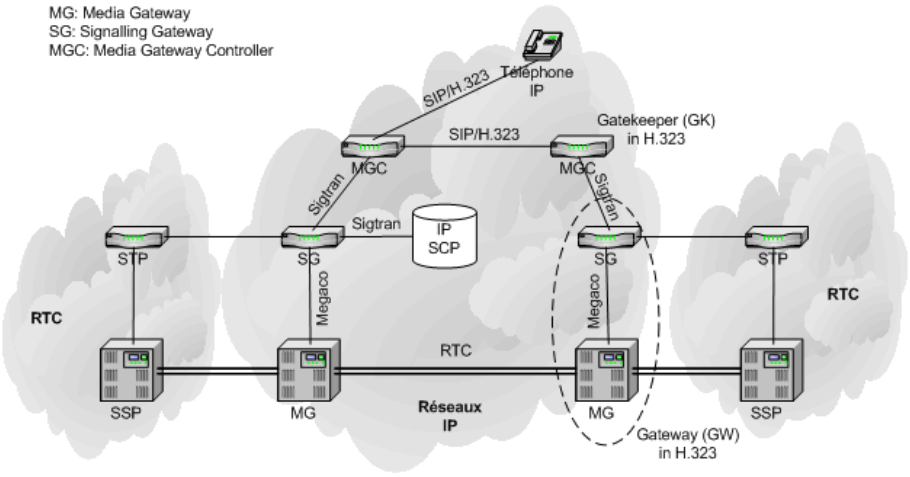


Figure 4 Architecture VoIP Sigtran

Plusieurs standards existent comme le H.323 de l'IUT ou l'IETF. Il semblerait que le dernier prenne l'ascension sur l'IUT. Voici une description brève de la pile de protocole proposée par l'IETF pour la VoIP.

- *Stream Control Transport Protocol (SCTP)* : Il s'agit ici du protocole SIGTRAN qui a la charge de transporter les messages SS7 entre les SG et les MGC, et entre un SG et un IP-SCP.
- *Megaco (H.248)* : Il s'agit du protocole de contrôle entre un MGC et des MG.
- *Session Initialtion Protocol (SIP)* : Assure le contrôle d'appels entre les MGC, ou entre des MGC et des téléphones IP.
- *Real Time Protocol (RTP)* : Transporte les paquets de voix.

La Figure 4 illustre un exemple typique d'architecture VoIP.

12.3.1. Failles Sécuritaires VoIP

La révolution VoIP est de pouvoir se passer de la structure propriétaire complexe des opérateurs de télécommunication à commutation de circuits. En effet, un opérateur VoIP peut éviter d'investir dans des commutateurs téléphoniques et les remplacer par des routeurs et des commutateurs réseaux moins onéreux, ce qui lui permet de proposer des tarifs très attractifs. Le pendant de cette approche est la vulgarisation des infrastructures nécessaires aux réseaux VoIP, ainsi que l'augmentation de la pénétration d'opérateurs virtuels. Avec cela augmentent aussi les risques d'intrusions dans un réseau, voire l'impersonnalisation d'un réseau. VoIP doit donc protéger son réseau de signalisation et de donnée, et n'est donc pas à l'abri d'attaques qui peuvent prendre des formes très variées que nous énumérons dans la suite de cette section.

- *Confidentialité* : La signalisation est aussi importante que la communication, étant donné que sa compromission permet à un intrus d'obtenir des informations importantes sur l'utilisateur. Par exemple, un SG compromis sera à l'origine de pistage d'appels ainsi que de création d'archives de communications passées par un utilisateur visé.
- *Ecoute* : La conversation en elle-même est aussi risquée si un MG est compromis. En effet, un intrus peut intercepter et modifier les paquets VoIP afin de pouvoir écouter les conversations.
- *Man in the Middle* : Les conversations VoIP sont aussi vulnérables vis-à-vis de ce genre d'attaque, en envisagent par exemple une interception d'une connexion et la modification des paramètres d'appels. Cette attaque est d'autant plus dangereuse qu'elle serait la source d'usurpations d'identité ou de redirections d'appels, le tout à l'insu de l'utilisateur.
- *Déni de Service* : Contrairement aux réseaux commutés par circuits, la disponibilité des ressources dans la VoIP n'est, en soit, jamais garantie. Il est tout à fait envisageable que des réseaux VoIP subissent des attaques de déni de service afin de rendre des éléments clés inopérationels.

- *Non répudiation* : Une fois qu'une destination accepte un appel, il est important d'avoir des mécanismes qui l'empêchent ensuite de nier l'avoir accepté.
- *Les terminaux et serveurs VoIP* sont aussi, de par leur nature informatique, très vulnérables à des attaques. En effet, il semble difficile de compromettre un téléphone analogique. En revanche, un téléphone VoIP contient principalement des logiciels qui peuvent être facilement modifiés.

12.3.2 Sécurisation de VoIP

Des solutions multiples ont été développées afin de sécuriser les réseaux VoIP. La première des solutions est évidemment la sécurisation de la signalisation. Devant être transportée à travers IP, la suite de protocoles Sigtran [SIG 99] a été développé pour les liens entre MGC et SG. L'emploi de SIP entre les MGSs reste cependant nécessaire. De plus, certains opérateurs VoIP utilisent des solutions propriétaires à la place de SIP ou SIGTRAN. Afin de sécuriser leurs messages, SIGTRAN ainsi que SIP se reposent sur respectivement IPSec et TLS. Pour une introduction compréhensible de Sigtran, nous référons le lecteur à [DAR 06].
Ensuite, il est important de sécuriser les conversations. Cela peut être effectué à l'aide de différents algorithmes de chiffrement, tels que IPSec ou Secured-RTP, qui offrent une confidentialité nécessaire, tout en réduisant la qualité des conversations dans des limites acceptables par les opérateurs et les utilisateurs. Dans le cadre de Secured-RTP, l'authentification des paquets peut être effectuée en employant MiKEY.
Cependant, l'emploi d'IPSec est problématique lorsque le trafic IP doit traverser des NAT comme illustré dans [IPV 06]. Cela ne pose aucun problème lorsqu'il n'y a qu'un utilisateur VoIP derrière un NAT, étant donné que le NAT échange une adresse privée par une adresse IP publique. En revanche, lorsqu'il y a de nombreuses sources IPSec derrière un NAT qui communiquent vers un serveur unique, la traduction des adresses IP devient problématique et produit une traduction asymétrique des adresses vers un seul utilisateur, de ce fait redirigeant le trafic vers un seul client VoIP. En conséquence, IPSec ne peut être utilisé lorsque de multiples utilisateurs VoIP au sein d'un même sous-réseau communiquent vers un même serveur à travers un NAT.
Il est finalement nécessaire de protéger les éléments du réseau VoIP. Des principes de protections similaires aux réseaux IP sont utilisés, comme le contrôle des ports, ou le contrôle d'accès aux routeurs, avec l'ajout de redondance pour protéger des éléments clés.
Le lecteur intéressé par une liste exhaustive des failles sécuritaires VoIP ainsi que des recommandations afin de les combler peut se référer à [DOS 06].

12.4. IP Multimedia Subsystem (IMS)

L'IP Multimedia Subsystem (IMS) est un nouveau standard des protocoles 3.5G, voire 4G, et constitue une évolution supplémentaire comparée à SIP. En effet, il fournit une couche intermédiaire au cœur des réseaux pour passer du mode appel classique (circuit) au mode session. IMS est basé en partie sur la signalisation SIP mais sa grande force est d'autoriser l'ouverture de plusieurs sessions en cours de communications. IMS peut être considéré comme un SIP intelligent, étant capable non seulement d'ouvrir des sessions multimédia, mais aussi y ajouter des règles de routage intelligentes afin de gérer l'appel en fonction de nouveaux paramètres comme la localisation, la présence ou le type de terminal. Créé initialement pour les réseaux cellulaires, IMS a été étendu aux réseaux sans fils (WLAN) et aux réseaux fixes en collaboration avec TISPAN. L'architecture IMS va donc incarner la convergence transparente entre le monde de la téléphonie mobile, fixe et le monde Internet.

12.4.1. Architecture IMS

IMS inclue une série de fonctions qui ne sont pas forcément distribuées par noeud. Il peut y avoir plusieurs fonctions dans un même système, ou une même fonction peut être distribuée dans plusieurs systèmes. Nous listons ici un résumé des diverses entités :

- *Serving Call Session Control Function (S-CSCF)* : Il s'agit du nœud central d'un réseau IMS et il est situé au point de passage de tous les messages de signalisation IMS. Il s'agit d'un serveur SIP, mais qui a aussi la charge du contrôle des sessions. Il est toujours localisé dans le réseau de base de l'utilisateur. Le S-CSCF utilise le protocole DIAMETER afin de contacter la base de donnée HSS de manière sécurisée afin d'obtenir des informations sur l'utilisateur.
- *Interrogating Call Session Control Function (I-CSCF)* : Il s'agit d'un Proxy SIP situé à la limite du domaine et joue le rôle de point d'accès dans le réseau de base de l'utilisateur. Il utilise le protocole DIAMETER afin d'interroger le HSS pour d'obtenir la localisation de l'utilisateur.
- *Proxy Call Sessions Control Function (P-CSCF)* : Il s'agit de la passerelle IMS et est aussi un Proxy SIP. Il a la charge d'authentifier l'utilisateur, et de mettre en place le protocole IPSec ESP en mode transport avec un utilisateur, assurant par là le contrôle d'accès et la protection des informations entrant sur le réseau IMS.
- *Media Resource Function (MRF)* : Il héberge les ressources multimédia dans le réseau de base de l'utilisateur.
- *Application Server Function (AS)* : Il héberge et exécute des services de télécommunications, comme les MMS, SMS, ou l'interception légale (LI).

- *Breakout Gateway Control Function (BGCF)* : Il s'agit d'un serveur SIP qui contient des fonctionnalités de routage pour les systèmes téléphoniques. Il est utilisé lorsqu'un utilisateur appelle un numéro de téléphone sur un réseau commutation par circuits (PSTN ou PLMN).
- *Home Suscriber Server (HSS)* : Il s'agit de la base de donnée principale qui informe les éléments IMS au sujet des appels et des sessions. Il est similaire à un HLR/AuC dans les réseaux GSM.

La Figure 5 illustre un exemple d'architecture typique entre un IMS d'origine et un IMS visité, mettant en communication un utilisateur UMTS et un PDA sur un WLAN.

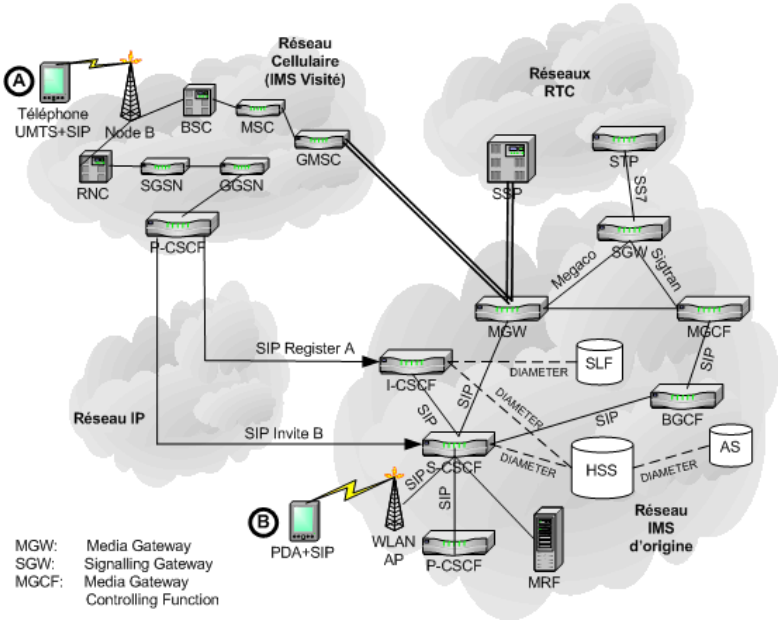


Figure 5 *Architecture d'IMS*

12.4.2 Sécurité dans IMS

A l'opposé de bien des solutions et protocoles proposés par le passé, IMS a été crée avec le soucis d'assurer une sécurité avancée. L'IMS AKA est cependant basé sur la sécurité assurée par *Secure SIP* et l'UMTS AKA. L'architecture de sécurité d'IMS peut être décomposé en celle du réseau cœur IMS et celle entre le P-CSCF et l'utilisateur.

12.4.2.1 Réseau Cœur IMS

L'architecture du réseau cœur IMS est similaire à celle recommandée par la norme 3GPP pour le réseau UMTS. Notamment

- *Confidentialité et Intégrité* : Les communications entre les différentes unités composant le réseau cœur IMS sont protégées par IPSec ESP en mode tunnel. De plus, les communications entre le HSS et les unités IMS s'effectuent en utilisant le protocole DIAMETER. Etant donné que toutes les unités d'IMS supportent SIP, ils incluent par défaut le protocole TLS. Il est donc aussi possible d'assurer la confidentialité et l'intégrité à l'aide de TLS dans le réseau cœur IMS à la place ou en complément d'IPSec. Les communications internes à un réseau coeur IMS ayant de faibles chances de traverser des NAT, le problème concernant IPSec illustré dans la section traitant VoIP ne s'applique pas.

12.4.2.2 Réseau Visité IMS

Lorsqu'un utilisateur accède à un réseau IMS hors de son réseau de base, il rentre en communication avec un P-CSCF. IMS fournit les systèmes de sécurisations suivants pour le lien entre l'utilisateur et le P-CSCF lors de l'accès IMS:

- *Authentification d'un utilisateur* : La souscription de l'utilisateur est authentifiée par le S-CSCF. Le mécanisme d'authentification est appelé IMS AKA et permet une authentification mutuelle entre l'utilisateur et le réseau de base (Home Network). La norme 3GPP recommande d'utiliser l'AKA UMTS comme mécanismes d'authentification et d'échange de clés. Le vecteur d'authentification est transporté par SIP et est obtenu de manière similaire à celui d'UMTS. La Figure 8 illustre un exemple d'authentification.
- *Ré-authentification d'un utilisateur* : Bien qu'un utilisateur soit toujours authentifié pendant l'enregistrement, le réseau IMS peut décider une nouvelle authentification en cours de session. Dans ce cas, le S-CSCF envoie un message de demande de re-authentification.
- *Confidentialité* : La confidentialité de l'identité de l'utilisateur est assurée en employant deux identifiant spécifiques à IMS, l'*IM Private Indentity (IMPI)* qui n'est stockée qu'à l'HSS et dans le module IM (ISIM) de l'USIM de l'utilisateur, et l'*IM Public Identity (IMPU)* qui est transmise sur le réseau. .La confidentialité de la signalisation SIP entre un utilisateur et le P-CSCF dépend de la politique de sécurité du réseau visité, mais la norme 3GPP recommande de rejeter l'accès à un utilisateur qui refuserait ou n'aurait pas la possibilité de chiffrer les communications. Les deux acteurs doivent négocier l'algorithme de chiffrement IPSec ESP employé entre *DES-EDE3-CBC* ou *AES-CBS*, et ensuite déterminer la clé de chiffrement CK^{exp} à partir d'une expansion de la clé CK générée pendant l'IMS AKA.

La norme 3GPP recommande la règle suivante :

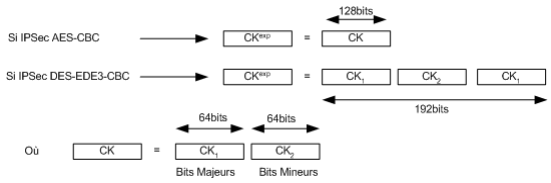


Figure 6 *Expansion de la clé de chiffrement CK*

- *Intégrité* : Afin de protéger les signaux SIP, un contrôle d'intégrité est implémenté entre l'utilisateur et le P-CSCF base sur IPSec ESP en mode transport. Premièrement, les deux acteurs doivent décider de l'algorithme à utiliser entre *HMAC-MD5-96* et *HMAC-SHA-1-96*. Ensuite, ils déterminent la clef d'intégrité IK^{exp} à partir d'une expansion de la clé IK générée pendant l'IMS AKA.
  La norme 3GPP recommande la règle suivante :

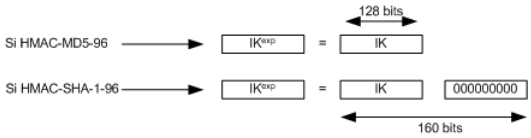
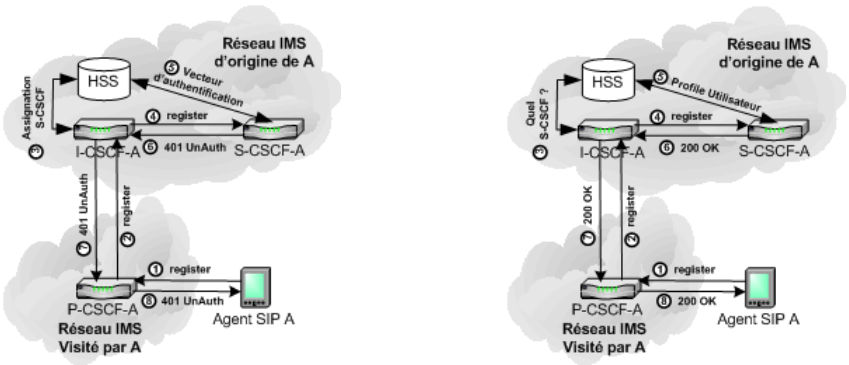


Figure 7 *Expansion de la clé d'intégrité IK*

La Figure 8 illustre le mécanisme en deux étapes d'enregistrement IMS, où la première phase lance un défi à l'utilisateur et où la seconde phase l'enregistre si le défi a été correct.



1 : IMS lance un défi à A *2 : IMS enregistre A*

Figure 8 Enregistrement en deux étapes d'IMS

La Figure 9 suivante illustre plus en détaille le mécanisme d'authentification et d'échange de clés IMS (IMS AKA). Notamment, on assume que les communications dans le réseau cœur IMS de base de l'utilisateur sont sécurisées par IPSec ESP en mode tunnel, et le mécanisme cryptographique de génération de clés est celui recommandé par la norme 3GPP pour l'UMTS. Le Proxy P-CSCF est le point d'accès d'un utilisateur, et il a donc la double charge d'authentifier l'utilisateur et d'établir des associations sécuritaires entre lui et l'utilisateur. Similairement à l'AKA UMTS, aucune clé secrète n'est transmise sur le lien entre le P-CSCF et l'utilisateur.

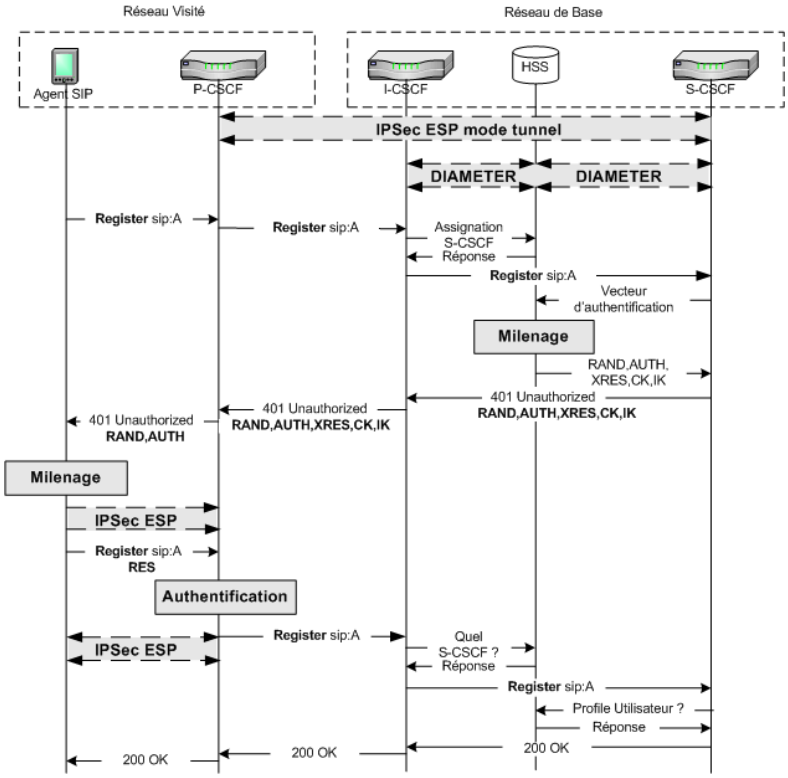


Figure 9 *IMS AKA*

Finalement, la Figure 10 suivante illustre le mécanisme de négociation d'algorithme de chiffrement et d'établissement d'associations sécuritaires entre le P-CSCF et l'utilisateur. Les deux unités échangent une liste des algorithmes qu'ils supportent afin de tomber sur une valeur commune. Dans le cas échéant, la norme 3GPP recommande de rejeter l'accès.

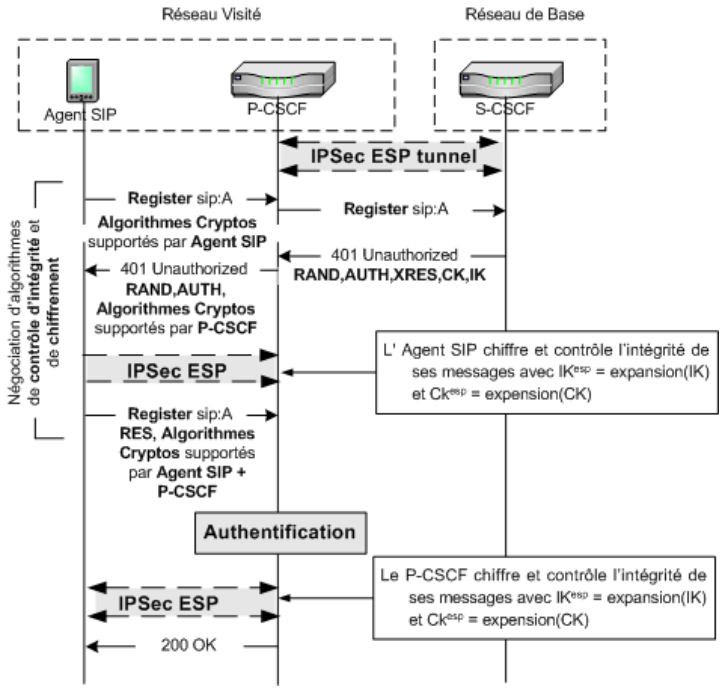


Figure 10 *Négociation de l'algorithme de chiffrement supporté dans IMS*

12.4.3 Failles Sécuritaires dans IMS

Malgré le soin apporté par la communauté 3GPP afin de sécuriser IMS, certaines failles existent toujours et sont énumérée dans la spécification IMS [IMS 06].

- Une version simplifiée d'IMS appelée *Early IMS* existe, et elle ne comprend pas certains systèmes de sécurités comme IPSec ou l'utilisation conjointe d'USIM et d'ISIM. Elle a été proposée dans un premier temps afin de simplifier son déploiement (équipements trop chers, trop complexe pour l'époque). Cette version IMS n'est pas sécurisée.
- *Ré-enregistrement par le mobile* : Si un mobile tente de se ré-enregistrer, il peut générer une attaque de type déni de service. En effet, lorsqu'il va tenter d'enregistrer un IMPU (Internet Multimedia Public Identity) qui est déjà enregistré et il répond avec une fausse réponse RES. En conséquence, le réseau IMS va supprimer la session attachée à l'IMPU.

- Un Utilisateur qui contacte directement le S-CSCF : Une fois qu'un utilisateur s'est correctement authentifié auprès d'un P-CSCF, un intrus peut tenter d'envoyer des messages SIP directement au S-CSCF. Cela veut dire que l'intrus passe outre le contrôle d'intégrité du P-CSCF. Cela peut générer les problèmes suivants :
    - Le contrôle de facturation ne peut plus être effectué (par le P-CSCF)
    - L'intrus ayant accès à S-CSCF peut envoyer des messages SIP « INVITE » ou « BYE » à d'autres utilisateurs, potentiellement interrompant leur communications, ou s'invitant à leurs communications.
    - Il peut jouer le rôle d'un P-CSCF

  Afin de lutter contre cela, les utilisateurs ne doivent pas pouvoir contacter le S-CSCF directement. Il faut aussi éviter l'IP spoofing des adresses sources SIP.

12.5. Sécurité 4G

Les réseaux dits de quatrième générations, aussi appelé NGN (Next Generation Networks), sont actuellement en cours de développements. Ils promettent un débit radio maximal inégalé à 100 Mb/s. Alors que la 3G a vu la naissance de l'hétérogénéité des réseaux avec une interconnexion IP, RTC et RMT, la 4G signifiera l'hétérogénéité du sous-système radio. Notamment, la superposition et la coopération des différentes technologies radio seront la révolution majeure du sous-système radio 4G. Par exemple, il est envisagé de faire collaborer un réseau WiFi avec un réseau cellulaire, sans interruption ni de communications ni de qualité de service.

Au niveau du sous-système réseau, l'ETSI avec TISPAN et le 3GPP avec IMS travaillent ensemble afin de définir un sous-système réseau incluant IMS comme axe central, et qui aura la charge d'assurer une pleine coopération entre les différents réseaux fixes et mobiles dans un environnement sécurisé tout IPv6, dans le but d'assurer des services multimédia aux utilisateurs. Evidemment, l'utilisateur n'aura pas à connaître la complexité technologique sous-jacente, mais le terminal aura la charge de choisir la meilleure technologie à utiliser en fonction de l'application demandée. Il est donc à envisager une plus grande coopérations entres les différents acteurs du monde des communications afin d'apporter aux utilisateurs des services de bonnes qualité dans un environnement sécurisé.

La Figure 11 illustre une vision schématique des réseaux 4G avec une segmentation en quatre parties - *utilisateur*, *accès*, *transport* et *service* - ainsi qu'une transparence des technologies et protocoles utilisés dans chaque segment.

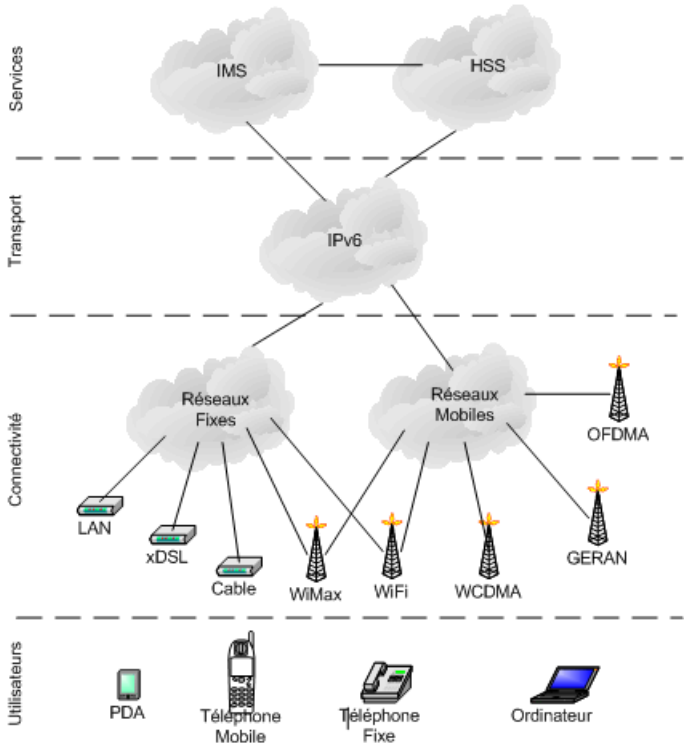


Figure 11 *Vision schématique de l'architecture 4G*

A ce jour, hormis les failles sécuritaires répertoriées pour IMS, la technologie 4G est trop récente pour en connaître ses points faibles. Il est évidemment imaginable qu'une telle hétérogénéite entre opérateurs réels ou virtuels générera très certainement des intrusions.
En revanche, le groupe de travail TISPAN a reconnu que la transmission à travers des NAT n'est pas traitée dans la norme 3GPP IMS [IMS 06]. Ils ont donc ajouté dans la version 7 [IMS 06] une option IPSec ESP UDP en mode tunnel permettant l'emploi d'IPSec ESP à travers des NATs, notamment entre un utilisateur et le P-CSCF. Pour plus de détails concernant l'interconnexion entre TISPAN et IMS, nous conseillons de se référer à la spécification 3GPP TISPAN [TIS 06].

12.6 Confidentialité

L'interconnexion des réseaux et leur (manque de) coopérations rendent complexe la gestion de la confidentialité. Des accords nationaux et internationaux ont été conclus afin de gérer la confidentialité des données des utilisateurs. Il est cependant

important de comprendre que, dans l'esprit actuel d'hétérogénéité des services et des réseaux de télécommunications, il est probablement impossible d'assurer cette confidentialité. La loi rend cependant les opérateurs responsables des fuites d'informations personnelles que leurs réseaux peuvent subir.

Pendant longtemps, les opérateurs se sont basé sur une approche de sécurité par obscurantisme, en utilisant des protocoles assumés sûrs mais qui, en fin de compte, ne l'étaient pas vraiment. Leur protection provenait de la faible diffusion de la connaissance de leurs réseaux internes et de leurs systèmes sécuritaires. Avec l'avènement de l'interconnexion des réseaux, de telles mesures ne sont donc plus envisageables. Des protocoles de sécurité beaucoup plus robuste ont donc été développés, rendant leur compromission plus du ressort de la cryptanalyse que de la réelle faille protocolaire. De plus, la complexité des algorithmes de chiffrement met à l'abri les opérateurs de télécommunication cellulaires. Une question peut donc se poser. Qu'en est-il de l'interception légale ?
L'interception légale est un mécanisme utilisé par toutes les agences de sécurité au monde afin d'obtenir plus ou moins légalement des informations, voire des communications, d'un ou plusieurs individus. Par le passé, la police, les services secrets et autres agences d'état ont utilisé les failles sécuritaire des opérateurs à leur profits. Par exemple, l'existence d'un « backdoor » pour déchiffrer des communications, ou la possibilité de s'identifier comme un réseau de communication et donc d'infiltrer d'autres individus, voire d'autres réseaux.
Cependant, avec la sécurisation accrue du monde des télécommunications actuel, ce genre d'interception est devenu très limité. Une parade a évidemment été proposée, ou plus précisément imposée. Il est exigé de pouvoir avoir accès aux réseaux des opérateurs quels qu'ils soient sur un territoire souverain par une injonction légale. En d'autres termes, des mécanismes doivent être mis en place par chaque opérateur afin de pouvoir suivre et pister des individus d'une manière centralisée et qui peut être accédé par une décision de justice. La nouvelle forme d'interception légale modifie notre vision du suivi de notre vie privée. En effet, on ne fait plus confiance aux mécanismes de sécurité afin d'assurer notre confidentialité mais plutôt à la justice de l'état souverain.
Le pendant de cette nouvelle forme de contrôle légal est la nécessité, dès la conception protocolaire, d'inclure des mesures d'interception légale. Le talon d'Achile de cette approche est la centralisation de la capacité d'interception. Cela crée une cible potentielle pour des tentatives d'intrusion sans dispositif légal.
D'un point de vue architecturel, une interception légale se fait par exemple en se callant sur une interface spéciale du MSC pour l'UMST et permet d'intercepter la signalisation et le trafic. Il est aussi possible d'avoir un suivit en temps réel de la consommation d'un utilisateur.

12.6.1. Terminologie

Plusieurs types d'interceptions légales ont été définis en fonction de la cible de l'interception.

- *Interception Réseau* : Type d'interception au niveau du point d'accès sans distinction d'utilisateur.
- *Interception Utilisateur* : Type d'interception d'un utilisateur en fonction de son identité cible. Un utilisateur peut avoir plusieurs identités au sein d'un réseau.
- *Interception Localisée* : Type d'interception limitée à une sous partie d'un réseau qui peut être soit orienté utilisateur soit réseau.

12.6.2. Protection des mécanismes d'interception

Dans les faits, les mécanismes d'interception fournissent une capacité d'interception totale des informations d'un utilisateur ou d'un élément de réseau. Il est donc nécessaire s'assurer la sécurité de ce « centre de commandement » de la vie privée des utilisateurs. Plusieurs mécanismes ont été proposés, non seulement afin de s'assurer qu'une agence de sécurité d'état ait accès à un opérateur, mais aussi que des opérateurs puissent vérifier l'identité de l'agence qui tente d'accéder à son réseau.

- *Interception flexible* : Il est notamment possible de désactiver l'interception, ou même de limiter cette interception dans les limites du cadre légal demandé.
- *Administration centralisée* : Seule la fonction administrative (ADMF) peut avoir accès aux interfaces d'interception sur les réseaux de télécommunications.
- *Confidentialité, Intégrité et Authentification* : Les communications entre les différentes interfaces d'interception et l'ADMF, et entre l'ADMF et l'agence d'état est assurée par, au minimum, des algorithmes tels que VPN ou CUG (Closed User Group).

La Figure 12 illustre le fonctionnement macroscopique des mécanismes d'interception. Nous recommandons aussi aux lecteurs intéressés par le domaine de l'interception légale de se référer à [INT 06] ou [AQS 05].

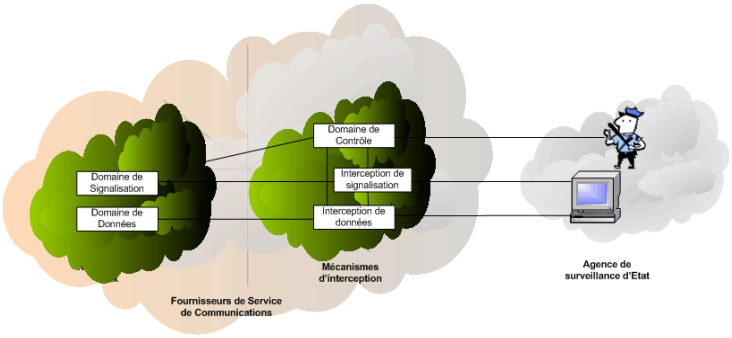


Figure 12 *Schéma de l'architecture d'interception légale*

12.7 Conclusion

Le monde des télécommunications a de cela intéressant qu'on a toujours été témoin d'une alternance entre les orientations des services téléphoniques mobiles et fixes. Le premier réseau intelligent (IN) fut, en son temps, le réseau GSM. Voyant son potentiel, les réseaux RTC les ont adaptés sur leurs réseaux SS7. De leurs succès commerciales, ces réseaux intelligents ont été étendu par les opérateurs fixes avant d'être à nouveaux adapté aux réseaux mobiles (p.ex. CAMEL).
Plus récemment, une vision similaire peut être faite avec l'évolution de SIP vers IMS et ses extensions, qui ont apporté une infrastructure transparente pour les services multimédia. Face à ce fort potentiel, et même avant le déploiement à large échelle d'IMS, les opérateurs de téléphonies fixes ont commencé à travailler sur une nouvelle architecture réseau appelée NGN (Next Generation Networks).
La convergence des réseaux de télécommunication est donc d'autant plus difficile qu'il y a différents opérateurs et consortiums de développement (IETF, IUT). Bien qu'on ait été témoin de multiples regroupements entre opérateurs fixes et mobiles ces dernières années, il a été plus raison d'une convergence commerciale que technologiques.

Devant cette difficulté de convergence totale, les préoccupations sécuritaires restent très sérieuses. IMS a apporté une avancée significative par rapport a SIP ou même SS7. IMS assure un contrôle d'accès entre les différents réseaux et utilisateurs, ainsi qu'aux services fournis. En revanche, il est illusoire de croire en un système de télécommunication grand public totalement sécurisé. Il est plus raisonnable d'envisage un système dont l'évaluation du potentiel des failles sécuritaires s'effectue en fonction d'un rapport entre les capacités techniques et financières pour les exploiter, avec la plus-value de l'objectif obtenu par son accès.
Nous pouvons citer l'exemple de la sécurisation des numéraux de carte de crédits lors de transactions financière. Il est parfois étonnant qu'autant de bruit soit fait

autour du danger de communiquer son numéro de carte de crédit à un fournisseur de service sur Internet, alors qu'il est commun de le donner à un opérateur pour un fournisseur de service sur la téléphonie fixe. Le potentiel de la plus value est identique, mais les faibles capacités techniques nécessaires à accéder aux paquets transmis sur un réseau IP par rapport à un réseaux propriétaire fixe ont justifié un chiffrement des transmissions.
On remarque donc que la réactivité des utilisateurs face à la sécurité de leurs données est principalement assurée par une relation de confiance entre un utilisateur, le fournisseur de service et le réseau acheminant le service. L'hétérogénéité des réseaux et des services ouvre donc la porte à de nombreuses failles dont le potentiel proviendra du succès des services offerts par ces réseaux de nouvelle génération.

12.8. Bibliographie

[SIP 02] IETF, "Session Initiation Protocol", RFC 3261.

[SSC 03] IETF, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", RFC 3329.

[NEW 06] Newport Networks, "SIP, Security and Session Controllers", White Paper, http://www.newport-networks.com/cust-docs/38-SIP-Security.pdf .

[IPV 06] Newport Networks, "IPSec in VoIP Networks", White Paper, http://www.newport-networks.com/cust-docs/91-IPSec-and-VoIP.pdf .

[SIG 99] IETF, "Framework Architecture for Signaling Transport", RFC 2719.

[DAR 06] Jim Darroch, "Introduction to Sigtran", *White Paper*, Artesyn Technologies, 2006.

[DOS 06] A. Doswald et al. "Best Practices for VoIP-SIP Security", Université de Genève, www.td.unige.ch/pdf/BP_VoIP_**Security**.pdf

[IMS 06] "3G Security: Access Security for IP based Services", 3GPP TS 33.203 version 7.3.0, 2006.

[TIS 06] "Protocols for Advanced Networking (TISPAN)", ETSI TS 182.006 v.1.1.1. 2006.

[INT 06] Newport Networks, "Lawful Intercept Overview", White Paper, http://www.newport-networks.com/cust-docs/87-Lawful-Intercept.pdf .

[AQS 05] AQSACOM, "White Paper on Interception of IP Networks", http://www.aqsacomna.com/us/articles/LI3GWhitePaperv4%2Epdf

12.9. Index