ANALYSE DES PROBLEMES ET DES SOLUTIONS DE SECURITE DE LA TELEPHONIE SUR IP

Ce chapitre a pour objectif d'analyser les principaux problèmes de sécurité de la téléphonie sur IP et les solutions proposées. Au travers des principales menaces rencontrées, nous présentons quels sont les techniques existantes pour s'en prémunir. L'analyse met en évidence les problèmes d'interopérabilité dus à l'hétérogénéité des réseaux et des protocoles de ToIP. Chaque système ayant ses propres mécanismes de sécurité, la sécurité de bout-en-bout des appels n'est actuellement pas considérée, sauf pour des usagers gouvernementaux. Seule une solution basée sur le canal média semble répondre à cette problématique.

2. Analyse des problèmes et des solutions de sécurité de la téléphonie sur IP

2.1. Cadre de la téléphonie sur IP : concepts, architectures et protocoles

2.1.1. *Le périmètre de l'analyse*

La téléphonie a connu ces dernières années une véritable révolution avec l'émergence de la téléphonie sur IP, qui apporte néanmoins certains inconvénients comme la problématique de la sécurité. La téléphonie sur IP cumule les vulnérabilités de la téléphonie classique et celles des réseaux informatiques. En déployant ou en adoptant une solution de ToIP, les entreprises et les particuliers exposent leurs systèmes à de nouvelles menaces. Le téléphone structurant très fortement notre manière d'échanger, la ToIP est une ouverture sur les données personnelles ou professionnelles. Par exemple, l'accès frauduleux à l'information au travers du téléphone est déjà une réalité pour les mafias qui ont organisé le marché noir d'informations issues des écoutes téléphoniques en Italie et en Grèce [CHA08].

Parallèlement, la ToIP correspond à une véritable transformation des télécommunications. La ligne téléphonique est dématérialisée, le service est dorénavant lié à un compte usager (caractérisé par identifiant et un mot de passe) auquel on associe des services comme la téléphonie, la visioconférence ou encore la messagerie. Tout cela est indépendamment du réseau d'accès ou de transport, de la localisation ou du type de terminal. L'utilisation d'un compte de ToIP sur un ordinateur d'hôtel pendant ses vacances permet certes de téléphoner à moindre coût, mais pose la question du stockage des données personnelles sur un équipement non maitrisé. La sécurité doit évidemment prendre en compte cette notion de mobilité.

Ainsi, la sécurité de la téléphonie constitue un domaine d'étude vaste. Ce chapitre va donc définir le périmètre de la ToIP et balayer l'ensemble des solutions existantes. Cette description a pour but de justifier la nature des solutions proposées par ce manuscrit.

Pour définir le périmètre de l'analyse, et par là même savoir où apporter les solutions de sécurité, il convient de définir les biens, les acteurs et les problèmes de la ToIP. La modélisation de la ToIP fournie par la figure 1 permet d'identifier les biens à protéger vis-à-vis des risques qui seront précisés ultérieurement. Cette vision abstraite caractérise deux grands domaines d'étude : le réseau et les échanges propres à la téléphonie. Deux sujets vont être développés dans ce chapitre :

- la sécurisation de la téléphonie au travers de l'architecture du réseau ;
- la sécurisation de la téléphonie au travers des choix protocolaires.

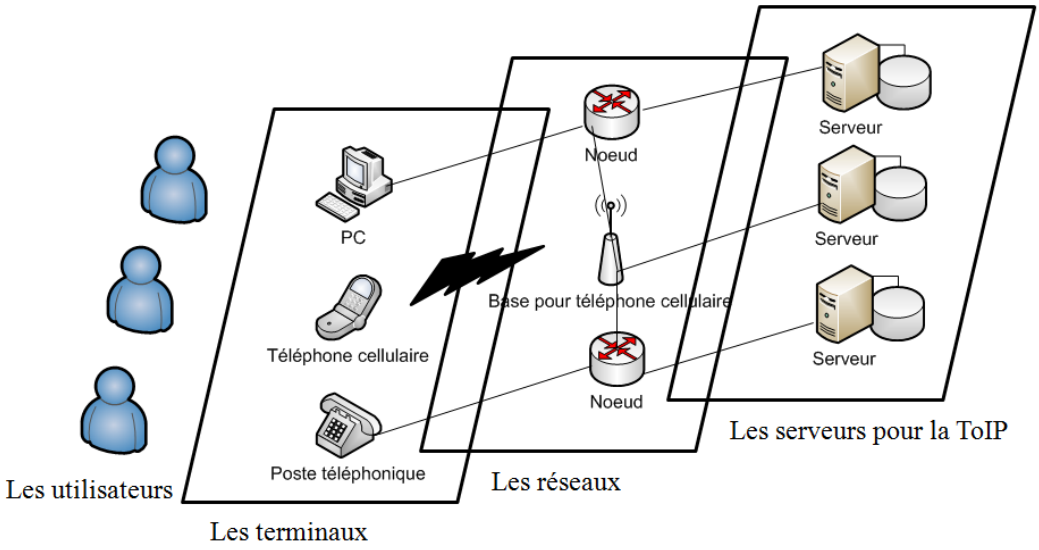

Figure 1. Architecture générique de la téléphonie sur IP

2.1.2. *Les éléments caractérisant une architecture de téléphonie sur IP*

Les infrastructures de téléphonie sur IP sont composées d'un ensemble d'équipements utilisant les technologies de l'Internet et de systèmes informatiques. Les usagers exploitent des terminaux interagissant avec différents types de serveur afin de gérer les comptes, la mobilité, la localisation et évidemment l'établissement de l'appel. Pour réaliser une telle infrastructure de téléphonie, de nombreux éléments matériels ou logiciels sont nécessaires comme :

- les autocommutateurs, qui permettent la création d'une liaison temporaire entre deux équipements de communication. Utilisés par exemple pour l'établissement d'une communication téléphonique, ces équipements sont appelés les IPBX[3] ;

[3] IPBX : Un IPBX est un PABX IP. Le terme PABX désigne un équipement qui permet de relier les postes téléphoniques d'un établissement (lignes internes) avec le réseau téléphonique public. Il permet en plus la mise en œuvre des services.

- les serveurs réseau comme : les serveurs DNS[4] ou encore les serveurs DHCP[5] ;
- les téléphones ou terminaux IP : équipement dédié à la téléphonie (hardphone) ou hébergeant un logiciel[6] de téléphonie (softphone) ;
- les routeurs : ce sont les équipements qui permettent l'aiguillage des paquets IP ;
- les cartes de commutations : elles jouent le rôle de passerelle avec les réseaux publics (RTC, GSM,…).

Le logiciel[7] est l'élément intelligent des équipements de ToIP. Il se retrouve dans les autocommutateurs (i.e. Asterisk [AST], 3CX [3CX]) et les téléphones (i.e. Twinkle [TWI], 3CX Phone [3CX]). Il permet à un équipement informatique de réaliser une fonction ou un service du monde des télécommunications. Il prend également en compte les spécificités de l'équipement d'accueil.

Les solutions issues des choix d'architecture du réseau seront évoquées dans ce mémoire mais ne feront pas l'objet d'une étude exhaustive. L'idée de notre étude n'est pas de lier la sécurité à l'infrastructure de téléphonie car, par définition, les appels doivent mettre en relation des personnes qui n'appartiennent pas forcément au même domaine ou qui ne sont pas reliés au même réseau local.

2.1.3. *Les protocoles de la téléphonie sur IP*

Un protocole est une formalisation permettant la communication entre plusieurs processus. En l'occurrence, un protocole de téléphonie doit permettre l'établissement d'une communication audio entre au moins deux personnes. Dans le monde de la ToIP, il existe une multitude de protocoles. SIP [RFC3261] est actuellement le plus populaire mais il faut également citer H323 [H323], SCCP (Skinny Client Control Protocol de Cisco) ou encore Skype [SKYPE].

Les protocoles de la ToIP se caractérisent par deux types de données :

- la signalisation qui décrit l'ensemble des échanges pour la gestion de l'appel, l'accès aux services et la négociation des paramètres pour le transport de la voix ;
- le flux vocal.

Les solutions de ToIP interopèrent globalement entre eux pour la gestion des appels. La continuité d'appel concerne principalement les fonctions de base de la signalisation et l'acheminement de la voix.

---

[4] DNS : Le Domain Name System (DNS) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine.

[5] DHCP : Dynamic Host Configuration Protocol est un protocole dont le rôle est d'assurer la configuration automatique des paramètres IP d'un terminal, notamment en lui assignant automatiquement une adresse IP.

[6] Téléphone logiciel : cet équipement est aussi appelé softphone. Un téléphone logiciel permet à un ordinateur muni d'un microphone et d'enceintes ou d'un casque audio d'établir un appel avec un autre téléphone en utilisant les services d'un serveur dédié à la téléphonie.

[7] Logiciel : un logiciel ou application est un ensemble de programmes qui permet à un système informatique d'assurer une tâche particulière.

2.2. Les risques et typologie des attaques

L'arrivée de la ToIP constitue de nouvelles opportunités d'attaques dans le monde des systèmes d'informations. La signalisation et la voix partageant le même réseau ou au moins les mêmes technologies que les réseaux de données IP, la téléphonie partage les mêmes vulnérabilités que les réseaux de données. A cela il faut rajouter les risques propres à la signalisation de la ToIP et au transport de la voix. Le tableau 1 fournit un premier niveau de description en précisant les différents risques liés à la téléphonie sur IP.

Tableau 1. Les principaux risques de la ToIP

Risques	Méthodes	Cibles
Déni de service Dos	Attaque entraînant l'indisponibilité d'un service/système pour les utilisateurs légitimes.	Un usager Un opérateur
Ecoute clandestine	Attaque permettant d'écouter l'ensemble du trafic de signalisation et/ou de la voix. Le trafic écouté n'est pas modifié.	Un usager
Détournement de trafic	Attaque permettant de détourner le trafic au profit de l'attaquant. Le détournement peut consister à rediriger un appel vers une personne illégitime ou à inclure une personne illégitime dans la conversation.	Un usager Un opérateur
Usurpation d'identité	Attaque basées sur la manipulation d'identité.	Un usager Un opérateur
Vols de services	Attaque permettant d'utiliser un service sans avoir à rémunérer son fournisseur.	Un usager Un opérateur
Communications indésirées SPIT[8] (SPAM téléphonique)	Attaque permettant à une personne de produire massivement des appels.	Un usager

L'autre manière de définir la menace est de caractériser les attaques. Ces dernières permettent à un élément menaçant d'exploiter une vulnérabilité. En synthétisant les travaux de [ZAR05], les attaques de la ToIP peuvent se ranger en trois grandes familles explicitées dans le tableau 2.

[8] SPIT : Spam over Internet Telephony. Tout comme un spam classique par courrier électronique, le SPIT peut être généré de manière similaire à partir de serveurs visant des millions d'utilisateurs de la ToIP. Le SPIT peut ralentir notablement le fonctionnement des architectures de téléphonie sur IP (exemple en engorgeant les boîtes vocales des usagers).

Tableau 2. Typologie des attaques

Type d'attaque	Principe du mode opératoire
Interception et modification	- Collecte d'informations sur les communications ; - Collecte d'informations sur les utilisateurs et le réseau ; - Manipulation du contenu des communications ; - Détournement des communications ; - Écoute des communications (conversation, message, vidéo).
Fraude et abus de service	- Usurpation d'identité ; - Contournement, porte dérobée (back door) ; - Manipulation des données de facturation.
Interruption de service ou déni de service	- Coupure physique ; - Épuisement des ressources ; - Déni de service général ; - Perte de courant.

Un certain nombre de contributions décrivent et analysent les attaques en ToIP [CHE09] [GUP07] [SNO]. Les réponses à ces risques passent par des solutions de sécurité, dont les propriétés seront définies ci-après.

2.3. Les différentes solutions

2.3.1. *Rappels des propriétés de sécurité*

Avant de présenter les solutions de sécurité, il convient de rappeler les définitions des propriétés de sécurité :

- **l'authentification** : garantir l'identité de l'usager qui envoie le message ;
    - dans le cadre de la ToIP, cette propriété permet par exemple à un serveur de vérifier qu'il fournit le service à l'usager légitime ;
- **la confidentialité** : rendre la conversation compréhensible aux personnes concernées uniquement ;
    - dans le cadre de la ToIP, cette propriété nécessite de chiffrer le flux audio ;
- **l'intégrité** : s'assurer que les données n'ont pas été modifiées entre l'envoi d'un message et sa réception ;
    - dans le cadre de la ToIP, cette propriété permet de s'assurer que les paramètres d'un appel n'ont pas été modifiés par une tierce partie ;

- **la non répudiation de l'appel** : la non répudiation des données nécessite l'archivage des données échangées ;
    - dans le cadre de la ToIP, cette propriété permet d'associer une communication à une personne de manière certaine ;
- **le non rejeu** : éviter de mémoriser puis de re-injecter les données dans le réseau ;
    - dans le cadre de la ToIP, cette propriété permet de ne pas pouvoir rejouer des échanges protocolaires par une personne tierce souhaitant accéder au service ;
- **l'anonymat** : capacité du système à masquer l'identité de l'usager ;
    - dans le cadre de la ToIP, cette propriété peut se traduire par le masquage de l'identité de l'appelant.

Ces propriétés de sécurité permettent de décrire les objectifs qu'il faut fixer pour protéger son système, compte tenu de ses besoins et des menaces. La formalisation de cette démarche s'appelle une analyse Sécurité des Systèmes d'Information (SSI). Il existe plusieurs méthodes pour définir le besoin de sécurité des systèmes d'informations comme EBIOS [EBIOS] (Expression des Besoins et Identification des Objectifs de Sécurité, cf. figure 2) ou MEHARI [MEH] (MEthode Harmonisée d'Analyse de Risques). L'objectif de toutes ces méthodes est de répondre au mieux à l'impératif de sécurité tout en prenant en compte le contexte et le besoin des utilisateurs. Le déroulement complet de l'analyse n'est pas dans le spectre de ce travail, en particulier l'analyse du besoin qui dépend que chaque utilisateur. Cependant, il est évident qu'une banque a besoin de plus de confidentialité qu'un centre d'appel, ce dernier demande quant à lui une forte disponibilité.

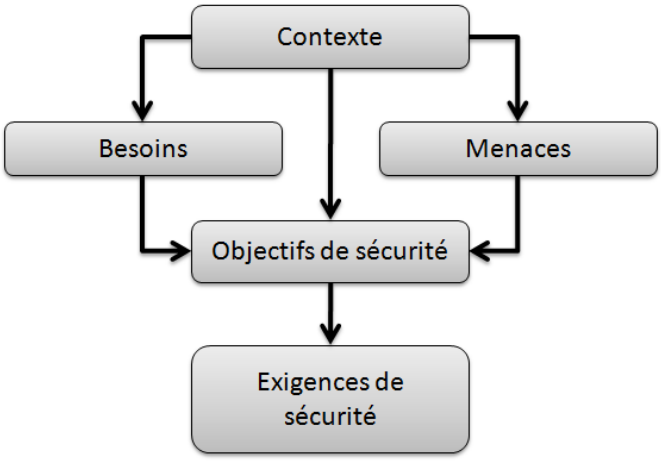

Figure 2. Principe de la méthode EBIOS

Les grandes entreprises utilisent en général ces méthodes pour la conception de leur système d'informations. Pour les particuliers ou les petites structures, il n'existe pas encore de réponse standard aux problèmes de sécurité de la téléphonie. Il semble cependant souhaitable de définir un besoin standard des particuliers pour faciliter l'adoption d'une solution unique de sécurité.

2.3.2. *Les principes de la sécurité de la téléphonique sur IP*

Les solutions pour sécuriser la ToIP existent. Elles font l'objet de recommandations formalisées par divers acteurs du domaine. Le document édité par le NIST[9] est une référence [KUH05]. Les méthodes de sécurisation usuelles s'appuient donc sur les 5 grands principes suivants :

- les bonnes pratiques ;
- la séparation des équipements voix/données ;
- l'authentification ;
- la confidentialité ;
- la sécurité périmètrique.

La sécurité physique est une partie essentielle de tout environnement sécurisé. Elle doit permettre de limiter l'accès aux locaux et donc aux équipements ainsi qu'aux données qu'ils contiennent. L'accès aux serveurs, aux équipements réseau et aux serveurs ToIP doit être restreint aux seules personnes autorisées. Les solutions dépendent du niveau de sécurité requis (pièces fermées, lecteurs de cartes, biométrie, etc.). L'objet de cette étude n'est pas d'étudier les moyens de protéger la téléphonie contre le vandalisme, les catastrophes naturelles ou encore les incendies. Néanmoins il est intéressant de retenir qu'une solution complète de sécurisation doit passer par une analyse fine et exhaustive. La suite de ce chapitre va donc se focaliser sur l'aspect réseau et protocole.

Avant de présenter les solutions de sécurité de la ToIP, rappelons les trois biens à protéger :

- l'infrastructure logiciel ou physique (serveur, téléphone,…) nécessaire pour recevoir et émettre des appels.
- la voix : la conversation téléphonique ;
- la signalisation : les informations nécessaires à l'établissement de l'appel ou aux services de téléphonie associés au compte usager.

2.3.3. *La sécurisation des architectures*

2.3.3.1. Les bonnes pratiques

La sécurité de la ToIP passe d'abord par l'application des bonnes pratiques. La ToIP faisant désormais partie intégrante des systèmes d'informations, les principes élémentaires s'appliquent donc pleinement.

[9] NIST : le National Institute of Standard and Technology dépend du ministère de l'économie américaine.

A titre d'illustration, nous citerons :

- prévoir des mesures générales :
    - politique de sécurité globale pour les systèmes de voix ;
    - formation et responsabilisation des utilisateurs et des administrateurs ;
    - redondance des équipements ;
    - étude des incidents ;
- tout système informatique étant susceptible de contenir des failles, une politique de mise à jour doit exister :
    - il est essentiel de maintenir à jour la version des logiciels grâce à un processus de management des mises à jour. Des mesures organisationnelles doivent être mises en place pour avoir des informations sur les équipements et les logiciels. Il faut pouvoir être certain d'être averti de la parution des versions et correctifs disponibles. Les évolutions doivent être testées avant d'être déployées ;
- désactiver les ports inutiles ;
- renouveler régulièrement les mots de passe des comptes utilisateurs ;
- prévoir des mots de passe longs et non triviaux ;
- définir l'utilisation des firewalls :
    - le firewall est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions. Il filtre les paquets de données échangés en analysant les entêtes. Les champs traités à minima sont les adresses IP de l'émetteur et du destinataire, les types de paquet transporté (UDP [RFC768], TCP [RFC793]) et le numéro de port associé.
- prévoir la suppression des comptes inutiles ;
- modifier les mots de passe par défaut des équipements ;
- vérifier les droits des utilisateurs ;
- prévoir le verrouillage des configurations (*) :
    - il convient que les usagers soient en mesure de modifier les paramètres de configuration de leur hardphone ou softphone ;
- définir le paramétrage par défaut des comptes (*) :
    - profil par défaut non-joignable depuis l'extérieur ;
    - profil par défaut ne pouvant pas faire suivre ses appels vers l'extérieur ;
    - auto-déconnexion la nuit ;
- contrôler les fonctionnalités de l'IPBX (*) :
    - vérifier les réglages de sécurité du serveur ;
    - définir une politique d'accès.

(*) : spécifique à la ToIP.

Cette liste n'est pas exhaustive mais elle illustre bien que la sécurité commence d'abord par des mesures simples. Les bonnes pratiques ne sont pas spécifiques à la ToIP mais contribuent à rendre son déploiement plus sain. Elles exigent des mesures organisationnelles rigoureuses pour maintenir le niveau de sécurité visé. De même, elles doivent être accompagnées d'une sensibilisation des usagers.

2.3.3.2. La séparation des équipements données et voix

Un des principes les plus recommandés pour protéger la ToIP est de séparer les équipements du réseau Data des équipements de l'infrastructure Voix. Cette séparation peut se faire de manière physique ou de manière logique. La séparation physique se traduit par deux réseaux différents avec des switches distincts. A ce choix relativement coûteux, il est préféré la séparation logique qui se décline de plusieurs manières :

- séparation des plages d'adresses IP : ce choix consiste à attribuer une plage d'adresses par réseau ; c'est-à-dire une plage pour le réseau données et une plage pour le réseau voix. Cette option nécessite que chaque réseau possède ses serveurs DHCP ou DNS ;

- séparation par VLAN[10] : cette fois, la séparation des équipements données et voix est obtenue par l'utilisation des VLAN. Il est même envisageable d'avoir des VLAN voix pour chaque catégorie d'équipements (hardphone, softphone, serveurs). Si les VLAN partagent des équipements, il est conseillé de les mettre dans une DMZ[11].

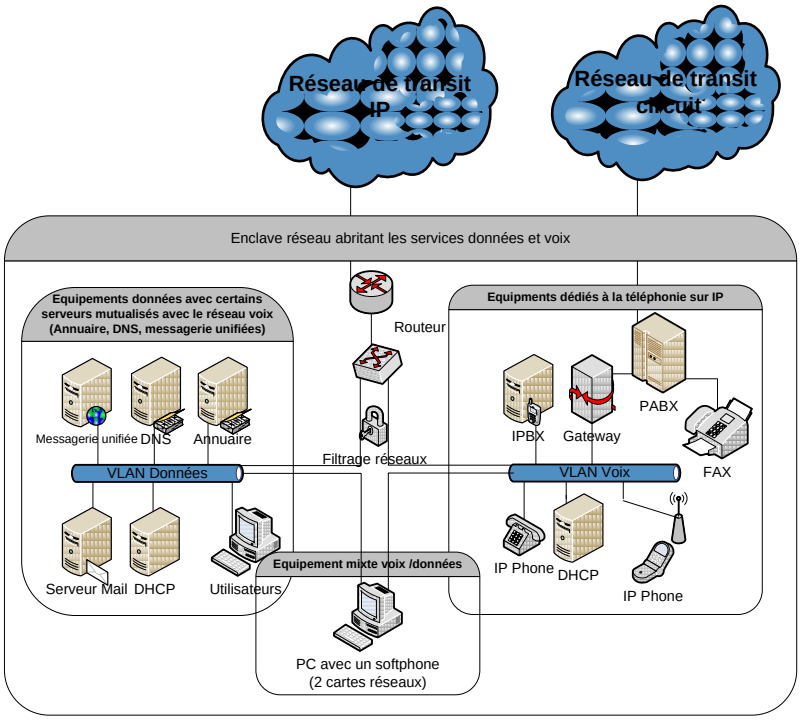

Figure 3. Architecture ToIP au sein d'une enclave type entreprise

[10] VLAN : un Virtual Local Area Network est une technique qui permet de créer un réseau local regroupant un ensemble de machines de façon logique et non physique.
[11] DMZ : en informatique, une zone démilitarisée (ou DMZ, de l'anglais demilitarized zone) est un sous-réseau isolé par un pare-feu. Ce sous-réseau contient des machines se situant entre un réseau interne et un réseau externe (typiquement, Internet). La DMZ permet à ses machines d'accéder à l'Internet et/ou de publier des services sur l'Internet sous le contrôle du pare-feu externe.

Les échanges entre les VLAN doivent être strictement contrôlés. Les équipements comme les switches ou les firewalls doivent permettre de filtrer les flux inter-VLAN. La figure 3 illustre ces recommandations pour une architecture VLAN voix et VLAN données sans serveurs mutualisés. Pour éviter de compromettre ce dispositif, il faut également penser à prendre des mesures de précautions sur les switches :

- désactiver les ports non-utilisés ;
- placer les ports inutilisés sur un VLAN inutilisé ;
- n'autoriser que les adresses MAC connues ;
- prévoir une authentification des machines.

La séparation logique des flux de voix et data est ainsi une mesure fortement recommandée. Elle doit permettre que les problèmes rencontrés sur un VLAN ne perturbent pas l'autre. L'objectif principal est bien une réduction du déni de service. D'autres dispositions sont également possibles pour renforcer la sécurité, en particulier pour limiter la possibilité de se connecter avec n'importe quelle machine sur le réseau. Les recommandations précédentes peuvent donc être complétées en mettant les ports inutiles dans un VLAN inutilisé, ou par la mise en place d'un contrôle d'accès sur l'adresse MAC et de mécanismes d'authentification.

2.3.3.3. L'authentification

L'authentification est la fonction de sécurité qui consiste à apporter et à contrôler la preuve de l'identité d'une entité (personne, message, logiciel,…). Compte tenu du périmètre de l'analyse, plusieurs mécanismes peuvent être envisagés, que ce soit au niveau réseau ou au niveau applicatif et donc dans les protocoles de ToIP. Concernant l'authentification au niveau protocolaire, ce point sera traité dans le paragraphe 2.3.4. et d'une manière plus détaillée pour SIP dans le chapitre 3.

Concernant les mécanismes d'authentification au niveau réseau, dans la mesure où la technologie IP est utilisée, les solutions usuelles de sécurité comme IPSec ou TLS peuvent répondre à l'objectif visé. Pour les équipements sans fil, les mécanismes utilisant EAP (Extensible Authentication Protocol) [RFC3748] peuvent être mis en place. Chaque couche porte ainsi sa solution de sécurité.

Généralement l'authentification est à sens unique, seul le terminal est authentifié. Ce constat est issu de modèle client/serveur dans lequel un client demande un accès à des services fournis par le serveur. Les protocoles de sécurité utilisés dans ces réseaux sont basés sur un processus type défi/réponse. Le serveur envoie un défi au client et ce dernier applique une fonction cryptographique sur le défi en utilisant un secret partagé (comme un mot de passe). Ainsi seul le client est authentifié. Cette approche ne suffit pas en ToIP. Dans la mesure où la signalisation porte des informations personnelles comme les destinataires des appels, il est plus qu'important que le client soit certain qu'il dialogue avec le serveur légitime. Cet objectif nécessite donc la mise en place d'une authentification dite « mutuelle ».

L'authentification doit également prendre en compte la mobilité. Les paramètres d'authentifications comme le mot de passe sont essentiels dans la robustesse du mécanisme. Utiliser un mot de passe sur un PC non maîtrisé est en soi une vulnérabilité. Il est essentiel de préserver ce secret. Ce sujet sera illustré dans le paragraphe 4.1.3.2.1.

2.3.3.4. La sécurité périmètrique

La sécurité périmètrique concerne les équipements placés aux frontières de l'infrastructure ToIP. Les éléments en périphérie assurent :

- la continuité des appels en permettant l'interopérabilité ou l'interconnexion ;
- éventuellement des propriétés de sécurité.

Il faut donc sécuriser les passerelles en utilisant les bonnes pratiques [§2.5.1.1.] voire en complétant le dispositif par des équipements spécifiques comme des firewalls ou des IDS (Intrusion Detection System). Rappelons que cette approche est lié à une infrastructure IP. Certes il existe des IDS dédiés à la ToIP comme le montre les travaux [NAS09]. Il convient néanmoins d'apporter des solutions de sécurité robuste dans la mise en œuvre du service téléphonique lui-même.

2.3.3.5. Confidentialité

Le chiffrement partiel ou total d'une information est nécessaire quand il existe un besoin de confidentialité. Ce besoin peut concerner la voix ou la signalisation. Concernant les couches transport ou réseau, les protocoles de sécurité usuels dans le mode de l'IP peuvent être mis à contribution pour sécuriser la ToIP. TLS et IPSec offrent un service de confidentialité. Plus largement, toutes les techniques VPN[12] peuvent permettre de protéger la voix et la signalisation entre deux sites. [DIA07] a comparé les différentes solutions et fait apparaître qu'IPSec est un bon candidat en termes de sécurité. Néanmoins les impacts sur les performances ne sont pas négligeables. Les implémentations méritent d'être optimisées. Comme nous le verrons dans le paragraphe 2.3.4, les deux principaux protocoles de la ToIP SIP et H323 préconisent l'emploi de chiffrement.

2.3.4. *La sécurisation des protocoles de téléphonie sur IP*

Les principaux protocoles de la ToIP, H323 et SIP, spécifient un cadre général pour la mise en œuvre de la sécurité. Cette dernière s'applique à la signalisation ou à la voix, voire aux deux. Les deux standards prévoient ou recommandent des mécanismes pour l'authentification, le chiffrement des données, le non-rejeu, l'anonymat et l'intégrité. Le protocole H323 se décompose en différentes recommandations qui portent chacune un ou plusieurs mécanismes de sécurité. L'authentification des usagers H323 est ainsi définie au travers de sa spécification RAS (Registration Admission Status) : l'authentification s'appuie alors sur un secret partagé ou un mécanisme à clé publique, voire après un

[12] VPN : Virtual Private Network (ou réseau privé virtuel) permet d'établir un lien sécurisé entre deux équipements.

échange de type Diffie Hellman[13]. Les modalités pour l'établissement et le contrôle d'appel peuvent être protégées au travers de la recommandation H.235 qui décrit le fonctionnement de H323 avec TLS ou IPSec. Ces protocoles peuvent alors fournir un service d'authentification, de confidentialité et d'intégrité des messages. De même SIP propose également des mécanismes de sécurité assez similaires qui seront présentés dans le chapitre 3, comme TLS ou encore IPSec. Concernant le média, les deux protocoles utilisent RTP [RFC3550] pour le transport de la voix. Le chiffrement de la communication est donc possible avec SRTP.

Les protocoles de la ToIP au travers de leurs spécifications comme SIP ou H323 reportent la sécurité sur le réseau en recommandant l'usage de TLS ou d'IPSec. Les limites de [§2.3.3.] se retrouvent alors au niveau des protocoles. Les propriétés de sécurité peuvent être très différentes d'un appel à l'autre. Il existe évidemment des mécanismes au niveau applicatif comme S/MIME pour SIP qui permet une solution de bout-en-bout en confidentialité, intégrité et une authentification mutuelle des usagers. Cette approche exige cependant que les deux terminaux implémentent les mêmes protocoles de ToIP avec les mêmes propriétés de sécurité. Or par essence, les interconnexions actuelles garantissent uniquement l'établissement de l'appel. Un usager utilisant SIP ne pourra donc pas établir un appel sécurisé de bout-en-bout avec un usager H323 à partir des spécifications des protocoles.

Ces solutions de sécurité rencontrent également de nombreuses difficultés d'implémentation et de déploiement. Le chiffrement de la signalisation ou de la voix [GUP07] nécessite un mécanisme de distribution de clés secrètes ou une infrastructure de gestion de certificats pour pouvoir être utilisé par tous les usagers ou les serveurs. Le chiffrement nécessite du temps de calcul et augmente la taille des paquets IP, ce qui n'est pas toujours conciliable avec une application temps réel comme pour le transport de la voix pour une communication. La multitude de protocoles comme SIP, H323 ou encore Skype ne facilite pas non plus l'adoption d'un standard de sécurité.

2.3.5. *La sécurité au niveau applicatif*

Fort du constat de [§2.3.4.], déjà avéré dans les années 80, la NSA[14] avait envisagé une solution de sécurité « universelle » appelée « Future Narrowband Digital Terminal » (FNBDT), permettant une sécurité de bout-en-bout. Après établissement de l'appel, le système met en œuvre une signalisation de sécurité dans le canal média. Depuis, le standard a évolué pour prendre en compte la technologie IP avec la version appelée « Secure Communications Interoperability Protocol » SCIP. Ce dernier est même devenu une norme aux Etats-Unis et à l'OTAN pour sécuriser la téléphonie. Il reste que cette approche, usuelle pour les militaires, reste marginale pour les particuliers.

---

[13] Diffie Hellmann : en cryptographie, l'échange de clés Diffie-Hellman, du nom de ses auteurs, est une méthode par laquelle deux entités peuvent se mettre d'accord sur un nombre (qu'ils peuvent utiliser comme clé pour chiffrer la conversation suivante) sans qu'une tierce personne puisse découvrir le nombre en écoutant les échanges. La sécurité de ce protocole réside dans le fondement mathématique de l'échange. [RFC2631] est une des applications.

[14] NSA : la National Security Agency est un organisme gouvernemental des États-Unis, responsable de la collecte et de l'analyse de toutes formes de communications.

La force de ce protocole est de ne faire aucune hypothèse sur le réseau sous-jacent. FNBDT fournit donc une architecture interopérable permettant de sécuriser des communications de bout-en-bout, quelque soit le réseau d'accès. Il faut néanmoins partager un équipement appelé STE (Secure Terminal Equipement). FNBDT n'est pas la seule solution applicative pour la sécurité de la ToIP mais il est le plus emblématique. Ce n'est pas non plus le premier protocole puisqu'il s'inscrit dans la continuité d'architectures plus anciennes comme SIGSALY[15].

FNBDT a inspiré les travaux [BAS05] de Carol Bassil qui a défini une architecture libre de sécurité applicative pour la voix sur IP. L'émergence d'une solution de sécurité robuste comme FNBDT ou SVSP n'a pas encore vu le jour pour les particuliers, car la perception du danger ne pousse pas encore à l'adoption de solutions de sécurité généralisées. Le monde des professionnels y vient comme le suggère [BEL09]. La sécurité de bout-en-bout des appels IP reste un sujet qui n'est pas traité systématiquement dans les architectures.

2.4. La typologie des méthodes pour sécuriser la téléphonie sur IP

De cette étude, nous proposons une typologie pour les solutions de sécurité. Les 5 grands principes pour sécuriser la ToIP sont :

- **sécuriser l'architecture** : c'est la première étape dans l'environnement des systèmes d'informations et de l'IP. L'application des bonnes pratiques est la première étape pour envisager toutes les autres solutions. Un softphone sur un PC sans anti-virus est exposé à toutes les attaques de l'Internet ;

- **sécuriser la signalisation** : dans le cas de SIP, cela revient à introduire des mécanismes comme S/MIME ou HTTP Digest. La sécurité est définie au moment de l'implémentation mais la continuité de service se limite aux domaines appliquant la politique de sécurité et utilisant le même protocole. Evidemment, il n'y a pas de continuité actuellement au changement de protocole pour permettre l'établissement de l'appel ;

- **sécuriser par extension** : il est (évidemment) toujours possible d'améliorer l'existant en rajoutant une en-tête ou d'appliquer de nouvelles méthodes de chiffrement, mais se pose alors le problème du déploiement et la gestion des différentes configurations. La compatibilité des différentes versions ne permettant pas d'imposer de nouvelles solutions. De même que précédemment cette approche ne s'applique qu'aux domaines ayant choisi cette solution ;

[15] SIGSALY : ce système est le premier système de télécommunications numériques. Il a été déployé par l'armée américaine en 1943 pour les communications entre les états-majors alliés. SIGSALY a été lancé sur la base d'un projet initié en 1942 pour pallier à l'insécurité des télécommunications analogiques brouillées et restituées en clair en temps réel par l'armée allemande. Reliant jusqu'à 12 stations lors de son retrait en 1946, son existence est restée secrète jusqu'en 1976.

- **sécuriser le canal média au moment de l'appel** : c'est le principe de SRTP. Cela nécessite que les protocoles de signalisation permettent la négociation de la clé de chiffrement ;

- **sécuriser d'une manière complètement transparente vis-à-vis du réseau** : les différentes infrastructures de ToIP interopèrent globalement entre eux pour la gestion des appels. La continuité concerne principalement les fonctions de base de la signalisation et l'acheminement de la voix. La sécurité est quant à elle propre à chaque infrastructure et ne fait l'objet d'aucune spécification au niveau des interconnexions. Faire abstraction du réseau permet donc d'envisager une solution bout-en-bout au niveau applicatif pour la sécurité : c'est l'approche de FNBDT, SCIP ou encore SVSP [§6.]. La solution de sécurité est mise en œuvre après l'établissement de l'appel dans le canal du média.

Chaque système portant ses propres mécanismes de sécurité, la sécurité de bout-en-bout des appels n'est actuellement pas considérée, sauf pour des usagers gouvernementaux ou dans le cas d'une homogénéité protocolaire entre deux usagers. Seule une solution basée sur le canal média semble répondre à cette problématique.

2.5. Méthodes et outils d'évaluation de la sécurité de la téléphonie sur IP

En complément des solutions pour sécuriser la ToIP, il existe deux processus complémentaires : l'audit et le fuzzing. Ces derniers n'apportent pas de solutions à proprement parler mais permettent de s'assurer que les mesures mises en place ne contiennent pas de failles et sont bien appliquées.

2.5.1. *L'audit*

L'audit n'est pas une technique propre à la ToIP. Il permet d'établir un diagnostic des services ou de solutions de sécurité mis en place dans l'entreprise ou l'organisme, et d'analyser les vulnérabilités en fonction de l'efficacité de ces services de sécurité. Cette démarche est essentielle pour vérifier que les mesures de sécurité sont bien appliquées, tant du point de vue organisationnel et que technique.

2.5.2. *Le fuzzing*

La deuxième méthode issue des systèmes d'informations qui peut s'appliquer à la ToIP est le fuzzing. Cette technique a émergé ces dernières années pour découvrir les vulnérabilités dans les implémentations logicielles et matérielles. Découlant du terme anglais fuzzy, signifiant flou ou brouillé, le fuzzing est une méthode s'appuyant sur des outils logiciels, des fuzzers, pour automatiser l'identification de bugs ou de failles dans des applications.

Le processus consiste à vérifier toutes les entrées possibles pour une application donnée, et à trouver les fonctionnements anormaux ou non conformes. Le fuzzer servira ainsi à bombarder l'application de codes volontairement malformés. L'opération se décompose en deux phases :

- générer des données aléatoires et/ou malveillantes ;
- injecter ces données dans l'application cible par ses divers canaux de communication et d'interaction.

Cette approche diffère de l'audit et des tests logiciels classiques en se focalisant sur les actions inattendues. La ToIP entre pleinement dans le spectre de cette approche. Des travaux ont d'ailleurs été menés sur cette problématique. Au travers d'un outil spécifique pour la voix sur IP appelé KIF (cf. figure 4), les auteurs de [ABD08] ont souligné l'intérêt de cette technique en montrant que de nombreux équipements de ToIP présentent des vulnérabilités.

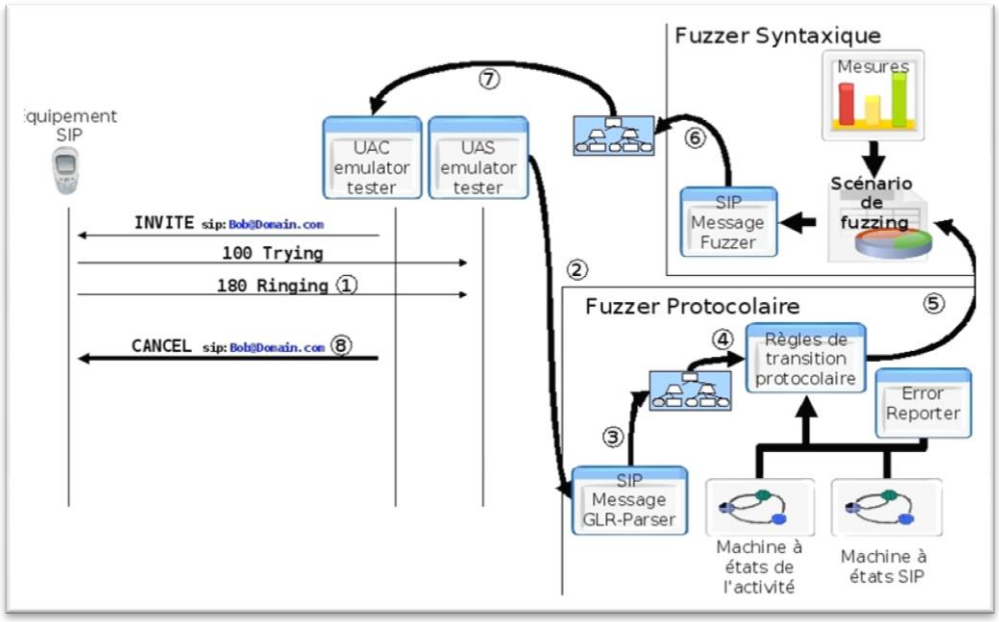

Figure 4. L'environnement de KIF [ABD08]

2.6. Conclusion

La sécurité de la téléphonie doit pouvoir répondre à trois grandes exigences : la disponibilité, l'intégrité et la confidentialité. D'autres propriétés comme l'authentification, le non-rejeu et la non-répudiation peuvent être également nécessaires. Chacune de ces exigences demande des mécanismes protocolaires ou des choix d'architecture bien particuliers. Les solutions de sécurité envisagées actuellement répondent à ces attentes mais ne tiennent cependant pas compte de la diversité des environnements de la téléphonie sur IP, sauf à considérer une solution dans le canal média comme avec FNBDT. Le contexte d'emploi des mécanismes de sécurité est souvent très restreint.

La sécurité n'est pas unifiée pour la téléphonie alors même que l'insécurité des SI augmente [LAD06]. Bien qu'il existe un consensus entre les différents opérateurs ou intégrateurs concernant la conception du réseau de téléphonie IP, il n'y a pas de standard universel pour la signalisation et donc pour la sécurité des appels de bout-en-bout. Ce constat milite pleinement pour la conception d'une solution de sécurité indépendante du réseau de transport. Cette approche ne traite cependant que partiellement le critère de

disponibilité mais permettra d'apporter confidentialité, authentification des entités et intégrité, voire plus si le contexte de l'appel le nécessite.

La fédération des solutions de sécurité viendra peut-être de l'adoption massive actuelle du standard SIP de l'IETF (Internet Engineering Task Force). Ce dernier spécifie la signalisation pour l'établissement d'un appel et les modalités pour le transport de la voix. Une large communauté a contribué à sécuriser l'environnement SIP, principalement en ajoutant de nouveaux paramètres ou en préconisant l'utilisation de protocoles de sécurité pour le transport des messages SIP ou de la voix. Ces propositions ont un coût en temps de calcul, en bande passante et ne sont pas toujours interopérables avec les implémentations existantes. Une sécurité de bout-en-bout des appels SIP reste encore à formaliser.

De facto, notre étude a recherché à renforcer la sécurité de l'existant, en particulier l'authentification, sans modifier les échanges de SIP pour faciliter l'adoption de nos solutions. L'objectif est de garantir une totale interopérabilité avec les infrastructures existantes tout en minimisant les impacts sur les performances de l'infrastructure de ToIP. Ce cahier des charges nous a permis de proposer des solutions innovantes et validées, en spécifiant une sémantique pour des valeurs aléatoires. Conscient que ces contributions sont un pis-aller, une définition d'une architecture de ToIP sécurisée est proposée dans le chapitre 6.