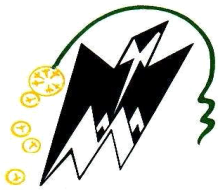
République Algérienne Démocratique et Populaire

Ministère de L'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri De Tizi-Ouzou



Faculté de Génie Electrique et d'Informatique

Département de l'Electronique

Mémoire de fin d'études

En vue de l'obtention Du Diplôme

De Master en Electronique

Option : Réseaux et Télécommunications

Thème :

Étude et Mise en place D'une Solution VoIP Sécurisée

Travail réalisé par :

Mr: Elyazid NOUREDDINE

Mr: Sid ali CHAFA

Proposé et dirigé par :

Mr: M. LAZRI

Mr: F. OUALOUCHE

Promotion: 2014

Remerciement

Au terme de ce travail, on tient à exprimer notre profonde gratitude et nos sincères remerciements à nos encadreurs Mr LAZRI et Mr OUALOUCHE pour leurs directives précieuses, et pour la qualité de leur suivi durant le travail effectuer pour ce projet.

On tient aussi à remercier vivement les membres du jury qui ont accepté d'évaluer notre projet. Nous leurs présentons toute nos gratitudes et nos profonds respects.

On souhaite exprimer enfin notre gratitude et nos vifs remerciements à nos familles et nos amis pour leurs soutiens.

Dédicace

Je voudrais dédier le présent travail à mes chers parents qui m'ont élevé et soutenu tout au long de ma vie, et tout spécialement à mon cher frère Sofiane béni thala

Je dédie également ce projet à mes chères sœurs et mes nièces : Miméne, Sérine et Lina.

Je tiens énormément à remercier mes chers amis et Camarades de ma promotion : Yazid, Bilka, Amine, Samir, fateh, Fariza, Kenza, Nassima et sans oublier Yazid si-3li, Madjid, Sofiane tsou tsou et Abderezak

Enfin, je voudrais dédier ce travail à toute personne ayant participé de loin ou de près à sa réalisation.

Chafa Sid Ali

Dédicace

Je remercie Dieu le tout puissant de m'avoir donné la force de réaliser ce projet.

Je voudrais dédier le présent travail à mes chers parents qui m'ont élevé et soutenu tout au long de ma vie, a mes deux sœurs Radia et Yasmine ainsi que toute ma famille au complet.

Je tiens énormément à remercier mes chers amis et camarades Amine, Yacine, Tarik, Sid Ali, sofiane et Mustapha.

Enfin, je voudrais dédier ce travail à toute personne ayant participé de loin ou de près à sa réalisation.

Noureddine Elyaziod

sommaire

Liste des figures

–

Introduction générale

La VoIP est aujourd'hui le nom d'une nouvelle technologie de télécommunications qui a radicalement transformé la notion d'appel téléphonique. VoIP est l'acronyme de Voice over Internet Protocol : voix sur le protocole Internet ou, plus simplement, "voix sur IP". C'est une application-phare du monde des Télécoms et notamment pour les entreprises.

A l'origine, déployée pour des raisons d'économies, son succès est largement dû aux services innovants et utiles pour l'entreprise qu'elle propose : communications unifiées, conférences multimédia, nomadisme, intégration SI, applications mobile...

Pour bénéficier de l'avantage du transport unique IP, introduire de nouveaux services voix et vidéo. Ce fût en 1996 la naissance de la première version voix sur IP appelée H323. Issu de l'organisation de standardisation européenne ITU-T sur la base de la signalisation voix RNIS (Q931), ce standard a maintenant donné suite à de nombreuses évolutions, quelques nouveaux standards prenant d'autres orientations technologiques.

Plusieurs fournisseurs offrent certaines solutions qui permettent aux entreprises de migrer vers le monde IP. Des constructeurs de PABX tels que Nortel, Siemens, et Alcatel préfèrent la solution de l'intégration progressive de la VoIP qui ne permet pas de bénéficier de tous les services et la bonne intégration vers le monde des données.
Le développement des PABXs software, est la solution proposée par des fournisseurs tels que Cisco et Asterisk. Cette approche permet de bénéficier d'une grande flexibilité, d'une très bonne intégration au monde des données et de voix, et surtout d'un prix beaucoup plus intéressant.
Cette solution, qui est totalement basée sur la technologie IP, est donc affectée par les vulnérabilités qui menacent la sécurité de ce protocole et l'infrastructure réseau sur laquelle elle est déployée. Cette dernière est le majeur problème pour les entreprises et un grand défi pour les développeurs. Certaines attaques sur les réseaux VoIP, comme

les attaques de déni de service (DoS). Pour cela la sécurité du réseau VoIP n'est pas seulement une nécessité mais plutôt une obligation, avec laquelle on peut réduire, au maximum, le risque d'attaques sur les réseaux VoIP.

Ce projet a pour objectif l'étude du réseau VoIP, ses protocoles, ses architectures et ses standards. Aussi, l'étude des vulnérabilités, des attaques de sécurité contre ce réseau, et la mise en place de la solution sécurisée (serveur Asterisk et client X-lite) font l'objet de ce travail.
Ce mémoire est structuré en quatre chapitres :

En premier chapitre nous introduisons la voix sur IP avec la présentation de ses éléments. Ensuite, nous décrivons ses architectures et protocoles en les expliquant, et une démonstration des points forts et faible de la VoIP.

Dans le deuxième chapitre, nous présentons la défaillance et les vulnérabilités ainsi que les attaques de sécurités possibles contre cette technologie avec des explications et définitions.

En troisième chapitre, nous réalisons l'installation et la configuration de la solution mise en place basée sur le serveur Asterisk avec le client X-lite et la configuration des différents paramètres.

En quatrième et dernier chapitre, nous mettons en place la réalisation d'une attaque sur le réseau. Ensuite une implémentation des différentes solutions et mesure nécessaire pour pouvoir contrer ces attaques.

Enfin, nous terminerons par une conclusion.

Chapitre I

Etude Générale de la voix sur IP

I.1 préambule

La voix sur IP est un terme qui désigne les protocoles, les logiciels et le matériel qui permettent la transmission de médias temps réel sous la forme de paquets.
La voix sur IP est devenue importante pour les entreprises. L'enjeu est de réussir à faire converger le réseau de données IP et le réseau téléphonique actuel.

Pour ce faire, dans ce chapitre, nous présentons quelques notions générales de la VoIP. D'abord, nous commençons par donner une définition de la voix sur IP. Ensuite nous présentons son fonctionnement ainsi les principaux protocoles VoIP

I.2 Définition

VoIP signifie Voice over Internet Protocol ou Voix sur IP. Comme son nom l'indique, la VoIP permet de transmettre des sons (en particulier la voix) dans des paquets IP circulant sur internet. La VoIP peut utiliser du matériel d'accélération pour réaliser ce but et peut aussi être utilisée en environnement de PC.

I.3 Architecture

La VoIP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Les trois principaux protocoles sont H.323, SIP et MGCP/MEGACO. Il existe donc plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP [03].

Certaines placent l'intelligence dans le réseau alors que d'autres préfèrent une approche égale à égale avec l'intelligence répartie à la périphérie. Chacune ayant ses avantages et ses inconvénients.

La figure I.1 décrit, de façon générale, la topologie d'un réseau de téléphonie IP.
Elle comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour

garantir une plus ou moins grande qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles ou contrôleur de commutation, appelées Gatekeeper. On retrouve les éléments communs suivants :

- **Le routeur** : permet d'aiguiller les données et le routage des paquets entre deux réseaux.

Certains routeurs permettent de simuler un Gatekeeper grâce à l'ajout de cartes spécialisées supportant les protocoles VoIP.

- **La passerelle** : permet d'interfacer le réseau commuté et le réseau IP.
- **Le PABX :** est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur, et le réseau téléphonique commuté (RTC). Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.
- **Les Terminaux :** sont généralement de type logiciel (software phone) ou matériel (hardphone), le softphone est installé dans le PC de l'utilisateur. L'interface audio peut-être un microphone et des haut-parleurs branchés sur la carte son, même si un casque est recommandé. Pour une meilleure clarté, un téléphone USB ou Bluetooth peut être utilisé.

Le hardphone est un téléphone IP qui utilise la technologie de la Voix sur IP pour permettre des appels téléphoniques sur un réseau IP tel que l'Internet au lieu de l'ordinaire système PSTN. Les appels peuvent parcourir par le réseau internet comme par un réseau privé.

Un terminal utilise des protocoles comme le SIP (Session Initiation Protocol) ou l'un des protocoles propriétaire tel que celui utilisée par Skype [03].

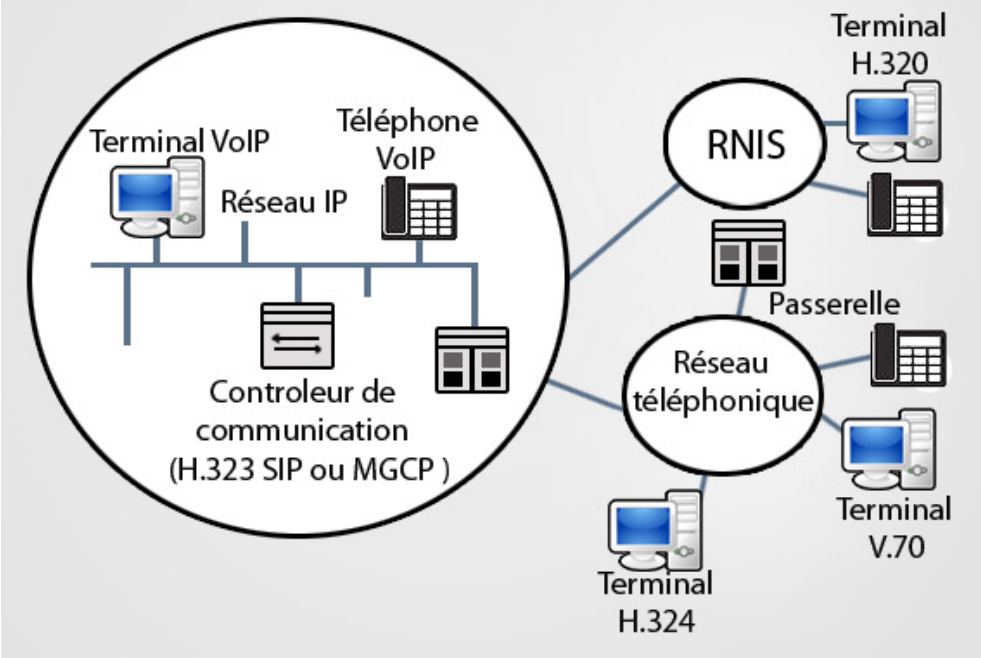


Figure I.1 : Architecture générale de la voix sur IP

La VoIP fonctionne par numérisation de la voix, puis par reconversion des paquets numériques en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format meilleur. Le signal numérique est plus tolérant au bruit que l'analogique.
Il existe plusieurs protocoles qui peuvent supporter la voix sur IP tel que le H.323, SIP et MGCP.

I.4 Principe de fonctionnement

La VoIP fonctionne par numérisation de la voix, puis par reconversion des paquets numériques en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format meilleur. Le signal numérique est plus tolérant au bruit que l'analogique.

Les réseaux TCP/IP sont des supports de circulation de paquets IP contenant un en-tête (pour contrôler la communication) et une charge utile pour transporter les données.

Les deux protocoles les plus utilisées actuellement dans les solutions VoIP présentes sur le marché sont le H.323 et le SIP.

I.5 Etude des protocoles H.323 et SIP

I.5.1 Protocole H.323

I.5.1.1 Description générale du protocole H.323

Le standard H.323 fournit, depuis son approbation en 1996, Il a été développé par l'ITU (International Télécommunications Union) pour les réseaux qui ne garantissent pas une qualité de service (QoS), tels qu'IP IPX sur Ethernet, Fast Ethernet et Token Ring. Il est présent dans plus de 30 produits et il concerne le contrôle des appels, la gestion multimédia, la gestion de la bande passante pour les conférences point-à-point et multipoints. H.323 traite également de l'interfaçage entre le LAN et les autres réseaux.

Le protocole H.323 fait partie de la série H.32x qui traite de la vidéoconférence a travers différents réseaux. Il inclue H.320 et H.324 liés aux réseaux ISDN (Integrated Service Data

Network) et PSTN (Public Switched Telephone Network).

Le protocole, H.323 crée une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information.

- Les messages de signalisation sont ceux envoyés pour demander la mise en relation de deux clients, qui indique que la ligne est occupée ou que le téléphone sonne, etc. En H.323, la signalisation s'appuie sur le protocole RAS pour l'enregistrement et l'authentification, et le protocole Q.931 pour l'initialisation et le contrôle d'appel.
- La négociation est utilisée pour se mettre d'accord sur la façon de coder les informations à échanger. Il est important que les téléphones (ou systèmes) utilisent un langage commun s'ils veulent se comprendre. Il s'agit du codec le moins gourmand en bande passante ou de celui qui offre la meilleure qualité. Il serait aussi préférable

d’avoir plusieurs alternatives de langages. Le protocole utilisé pour la négociation de codec est le H.245.

• Le transport de l’information s’appuie sur le protocole RTP qui transporte la voix, la vidéo ou les données numérisées par les codecs. Les messages RTCP peuvent être utilisés pour le contrôle de la qualité, ou la renégociation des codecs si, par exemple, la bande passante diminue.

Une communication H.323 se déroule en cinq phases :

- l’établissement d'appel.
- l’échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource réservation Protocol).
- l’établissement de la communication audio-visuelle.
- l’invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.)
- la libération de l'appel.

L'infrastructure H.323 repose sur quatre composants principaux :

- Les terminaux.
- Les Gateways.
- Les Gatekeepers.
- Les MCU (Multipoint Control Units).

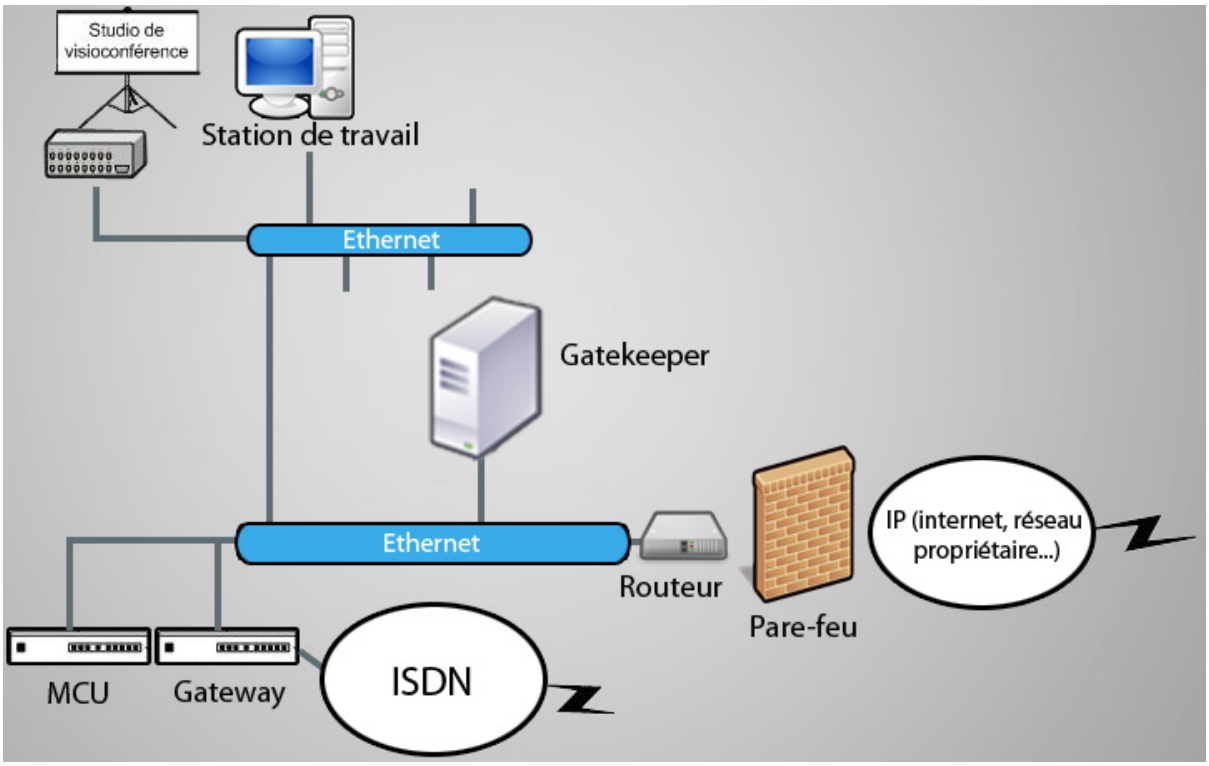


Figure I.2 : Les composants de l'architecture H.323

I.5.1.2 Rôle des composants

• Les terminaux H.323

Le terminal peut être un ordinateur, un combiné téléphonique, un terminal spécialisé pour la vidéoconférence ou encore un télécopieur sur Internet. Le minimum imposé par H.323 est qu'il mette en œuvre la norme de compression de la parole G.711, qu'il utilise le protocole H.245 pour la négociation de l'ouverture d'un canal et l'établissement des paramètres de la communication, ainsi que le protocole de signalisation Q.931 pour l'établissement et l'arrêt des communications.

Le terminal possède également des fonctions optionnelles, notamment, pour le travail en groupe et le partage des documents. Il existe deux types de terminaux H.323, l'un de haute qualité (pour une utilisation sur LAN), l'autre optimisé pour de petites largeurs de bandes (28,8/33,6 kbit/s –G.723.1 et H.263) [08].

- **Gateway ou les passerelles vers des réseaux classiques (RTC, RNIS, etc.)**

Les passerelles H.323 assurent l'interconnexion avec les autres réseaux, ex:(H.320/RNIS), les modems H.324, téléphones classiques, etc. Elles assurent la correspondance de signalisation de Q.931, la correspondance des signaux de contrôle et la cohésion entre les médias (multiplexage, correspondance des débits, transcodage audio).

- **Gatekeeper ou les portiers**

Dans la norme H323, Le Gatekeeper est le point d'entrée au réseau pour un client H.323.

Il définit une zone sur le réseau, appelée zone H.323 (voir figure I.3 ci-dessous), regroupant plusieurs terminaux, Gateways et MCU dont il gère le trafic, le routage LAN, et l'allocation de la bande passante. Les clients ou les Gateway s'enregistrent auprès du Gatekeeper dès l'activation de celui-ci, ce qui leur permet de retrouver n'importe quel autre utilisateur à travers son identifiant fixe obtenu auprès de son Gatekeeper de rattachement.

Le Gatekeeper a pour fonction :

✓ La translation des alias H.323 vers des adresses IP, selon les spécifications RAS (Registration/Admission/Status) ;

✓ Le contrôle d'accès, en interdisant les utilisateurs et les sessions non autorisés

✓ Et la gestion de la bande passante, permettant à l'administrateur du réseau de limiter le nombre de visioconférences simultanées. Concrètement une fraction de la bande passante est allouée à la visioconférence pour ne pas gêner les applications critiques sur le LAN et le support des conférences multipoint
adhoc.

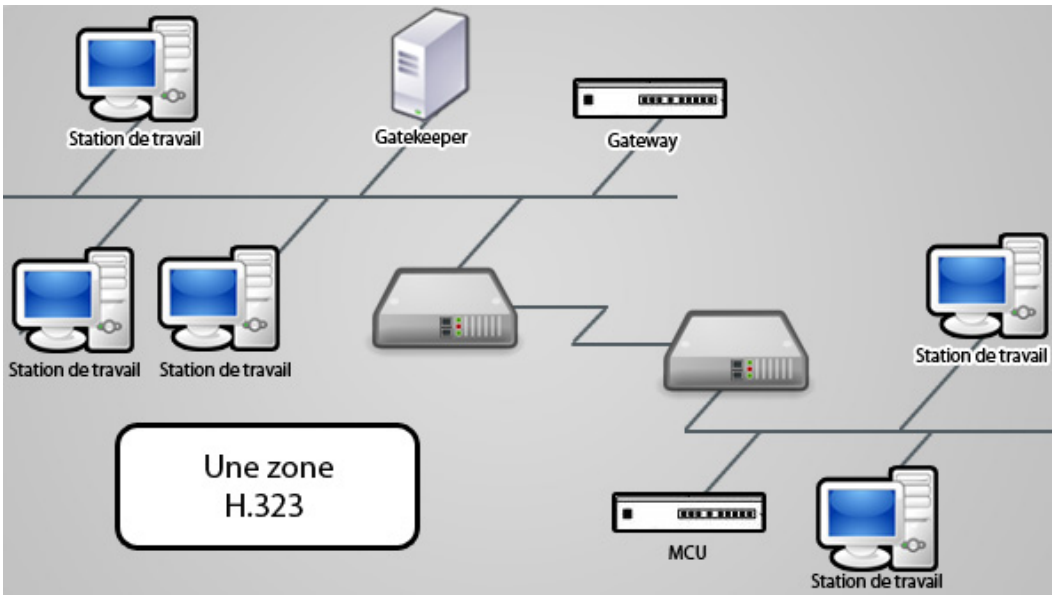


Figure I.3 : La zone H.323

• **Les MCU**

Les contrôleurs multipoint appelés MCU (Multipoint Control Unit) offrent aux utilisateurs la possibilité de faire des visioconférences à trois terminaux et plus en « présence continue » ou en « activation à la voix ». Une MCU consiste en un Contrôleur Multipoint (MC), auquel est rajouté un ou plusieurs Processeurs Multipoints (MP). Le MC prend en charge les négociations H.245 entre tous les terminaux pour harmoniser les paramètres audio et vidéo de chacun. Il contrôle également les ressources utilisées et plusieurs MP distribués sur le réseau et faisant partie d'autres MCU.

I.5.1.3 Avantages et inconvénients de la technologie H323

La technologie H.323 possède des avantages et des inconvénients. Parmi les avantages, nous citons :

• **Gestion de la bande passante** : H.323 permet une bonne gestion de la bande passante en posant des limites au flux audio/vidéo afin d'assurer le bon fonctionnement des applications critiques sur le LAN. Chaque terminal H.323 peut procéder à

l'ajustement de la bande passante et la modification du débit en fonction du comportement du réseau en temps réel (latence, perte de paquets et gigue).

- **Support Multipoint** : H.323 permet de faire des conférences multipoint via une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc.
- **Support Multicast** : H.323 permet également de faire des transmissions en
- **Interopérabilité *:*** H.323 permet aux utilisateurs de ne pas se préoccuper de la manière dont se font les communications, les paramètres (les codecs, le débit…) sont négociés de manière transparente.
- **Flexibilité :** une conférence H.323 peut inclure des terminaux hétérogènes (studio de visioconférence, PC, téléphones…) qui peuvent partager selon le cas, de la voix de la vidéo et même des données grâce aux spécifications T.120.

Les inconvénients de la technologie H.323 sont :

- La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la convergence des services de téléphonie et d'Internet, ainsi qu'un manque de modularité et de souplesse.
- Comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité [08].

I.5.2 Protocole SIP

I.5.2.1 Description générale du protocole SIP

Le protocole SIP (Session Initiation Protocol) est un protocole normalisé et standardisé par l'IETF (décrit par le RFC 3261 qui rend obsolète le RFC 2543, et complété par le RFC 3265) qui a été conçu pour établir, modifier et terminer des sessions multimédia. Il se charge de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de média utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol). SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. SIP tant indépendant de la transmission des données, tout type de données et de protocoles peut être utilisé pour cet échange [05].

SIP est le standard ouvert de VoIP, interopérable, le plus étendu et vise à devenir le standard des télécommunications multimédia (son, image, etc.). Skype par exemple, qui utilise un format propriétaire, ne permet pas l'interopérabilité avec un autre réseau de voix sur IP et ne fournit que des passerelles payantes vers la téléphonie standard. SIP n'est donc pas seulement destiné à la VoIP mais pour de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo.

I.5.2.2 Principe de fonctionnement

Le protocole SIP se base sur les différents aspects et caractéristiques qui le forment.
Les principales caractéristiques de ce protocole sont :

- **Fixation d'un compte SIP**

Il est important de s'assurer que la personne appelée soit toujours joignable. Pour cela, un compte SIP sera associé à un nom unique. Par exemple, si un utilisateur d'un service de voix sur IP dispose d'un compte SIP et que chaque fois qu'il redémarre son ordinateur, son adresse IP change, il doit cependant toujours être joignable. Son compte SIP doit donc être associé à un serveur SIP (proxy SIP) dont l'adresse IP est fixe. Ce serveur lui allouera un compte et il permettra d'effectuer ou de recevoir des appels quelques soit son emplacement. Ce compte sera identifiable via son nom (ou pseudo).

- **Changement des caractéristiques durant une session**

Un utilisateur doit pouvoir modifier les caractéristiques d'un appel en cours. Par exemple, un appel initialement configuré en (voix uniquement) peut être modifié en (voix + vidéo).

- **Différents modes de communication**

Avec SIP, les utilisateurs qui ouvrent une session peuvent communiquer en mode point à point, en mode diffusif ou dans un mode combinant ceux-ci [09].

Mode Point à point : on parle dans ce cas-là d'«unicast » qui correspond à la communication entre deux machines.

Mode diffusif : on parle dans ce cas-là de « multicast » (plusieurs utilisateurs via une unité de contrôle MCU – Multipoint Control Unit).

Combinatoire : combine les deux modes précédents. Plusieurs utilisateurs interconnectés en multicast via un réseau à maillage complet de connexion.

- **Gestion des participants**

Durant une session d'appel, de nouveaux participants peuvent joindre les participants d'une session déjà ouverte en participant directement, en étant transférés ou en étant mis en attente (cette particularité rejoint les fonctionnalités d'un PABX par exemple, où l'appelant peut être transféré vers un numéro donné ou être mis en attente).

- **Négociation des médias supportés**

Cela permet à un groupe durant un appel de négocier sur les types de médias supportés.

Par exemple, la vidéo peut être ou ne pas être supportée lors d'une session.

- **Adressage**

Les utilisateurs disposant d'un numéro (compte) SIP disposent d'une adresse ressemblant à une adresse mail (sip:numéro@serveursip.com). Le numéro SIP est unique pour chaque utilisateur.

- **Modèle d'échange**

Le protocole SIP repose sur un modèle Requête/Réponse. Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes. La liste des requêtes échangées est la suivante :

Invite : cette requête indique que l'application (ou utilisateur) correspondante à l'url SIP spécifié est invité à participer à une session.

Ack : cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête Invite.

Options : un proxy server en mesure de contacter l'UAS (terminal) appelé, doit répondre à une requête Options en précisant ses capacités à contacter le même terminal.

Bye : cette requête est utilisée par le terminal de l'appelé à fin de signaler qu'il souhaite mettre un terme à la session.

Cancel : cette requête est envoyée par un terminal ou un proxy server à fin d'annuler une requête non validée par une réponse finale.

Register : cette méthode est utilisée par le client pour enregistrer l'adresse listée dans l'URL TO par le serveur auquel il est relié.

- **Codes d'erreurs**

Une réponse à une requête est caractérisée, par un code et un motif, appelés respectivement code d'état et raison phrase. Un code d'état est un entier codé sur 3 digits indiquant un résultat à l'issue de la réception d'une requête. Ce résultat est précisé par une phrase, text-based (UTF-8), expliquant le motif du refus ou de l'acceptation de la requête. Le code d'état est donc destiné à l'automate gérant l'établissement des sessions SIP et les motifs aux programmeurs. Il existe 6 classes de réponses et donc de codes d'état, représentées par le premier digit :

- 1xx = Information - La requête a été reçue et continue à être traitée.
- 2xx = Succès - L'action a été reçue avec succès, comprise et acceptée.
- 3xx = Redirection - Une autre action doit être menée afin de valider la requête.
- 4xx = Erreur du client - La requête contient une syntaxe erronée ou ne peut pas être traitée par ce serveur.
- 5xx = Erreur du serveur - Le serveur n'a pas réussi à traiter une requête apparemment correcte.
- 6xx = Echec général - La requête ne peut être traitée par aucun serveur.

I.5.2.3 Rôle des composants

Dans un système SIP on trouve deux types de composantes, les agents utilisateurs (UAS, UAC) et un réseau de serveurs (Registrar, Proxy).

L'**UAS** (User Agent Server) représente l'agent de la partie appelée. C'est une application de type serveur qui contacte l'utilisateur lorsqu'une requête SIP est reçue. Et elle renvoie une réponse au nom de l'utilisateur.

L'**U.A.C** (User Agent Client) représente l'agent de la partie appelante. C'est une application de type client qui initie les requêtes.

Le **Registrar** est un serveur qui gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données (figureI.4).

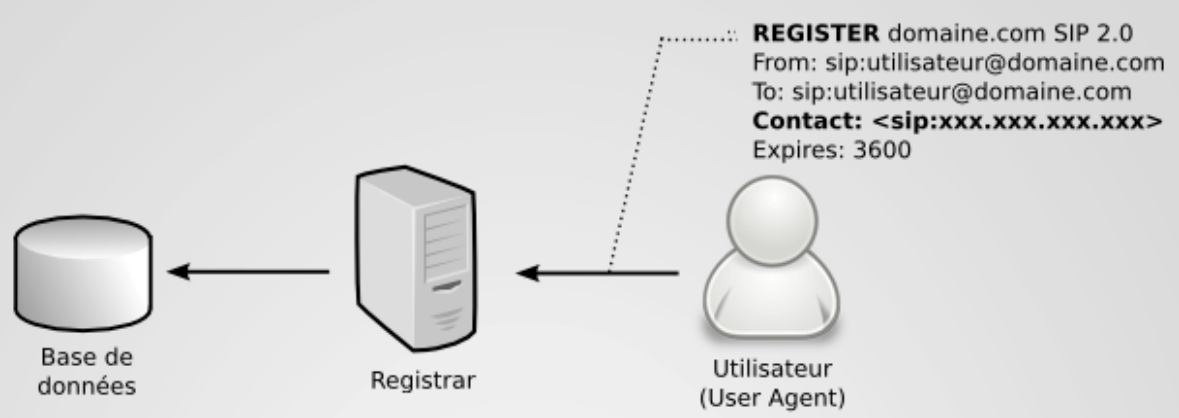


Figure I.4 : Enregistrement d'un utilisateur

Un **Proxy SIP** sert d'être l'intermédiaire entre deux User Agents qui ne connaissent pas leurs emplacements respectifs (adresse IP). En effet, l'association URI-Adresse IP a été stockée préalablement dans une base de données par un Registrar. Le Proxy peut donc interroger cette base de données pour diriger les messages vers le destinataire. La figure I.5 montre les étapes de l'interrogation du proxy la base de données.

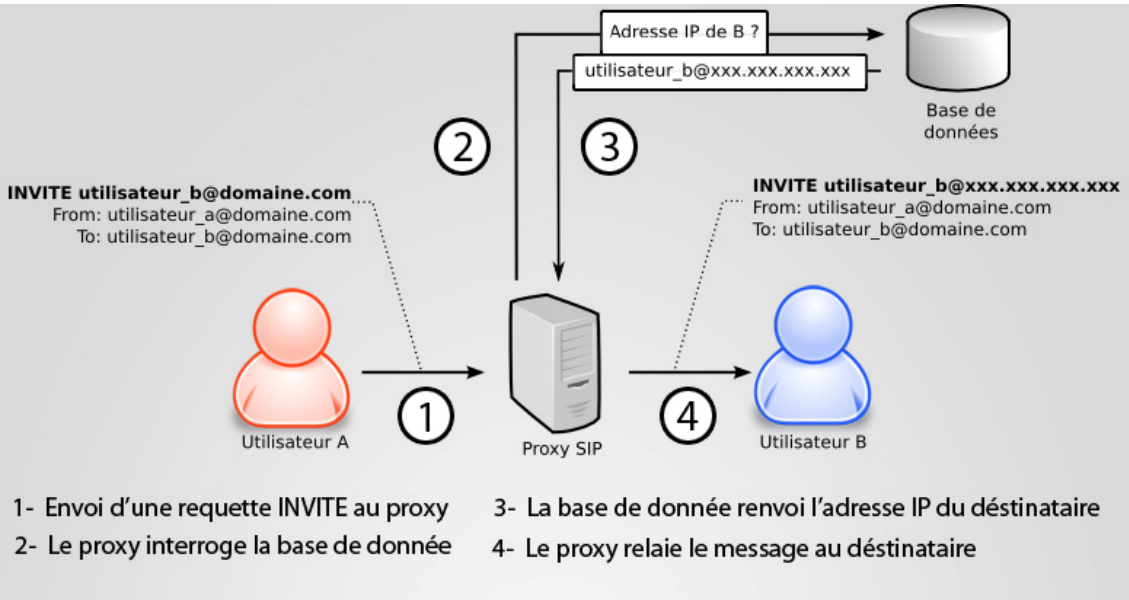


Figure I.5 : Principe du protocole SIP

I.5.2.4 Avantages et inconvénients

Ouvert, standard, simple et flexible sont les principales atouts du protocole SIP, voilà en détails ces différents avantages :

- Ouvert : les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.
- Standard : l'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP.
- Simple : SIP est simple et très similaire à http.
- Flexible : SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle, etc.).
- Téléphonie sur réseaux publics : il existe de nombreuses passerelles (services payants) vers le réseau public de téléphonie (RTC, GSM, etc.) permettant d'émettre ou de recevoir des appels vocaux.
- Points communs avec H323 : l'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.

Par contre une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du

trafic superflu sur le réseau. Un autre inconvénient est le faible nombre d'utilisateurs : SIP est encore peu connu et utilisé par le grand public, n'ayant pas atteint une masse critique, il ne bénéficie pas de l'effet réseau [09].

I.6 Comparaison des deux protocoles H-323 et SIP

Les deux protocoles SIP et H323 représentent les standards définis jusqu'à présent pour la signalisation à propos de la téléphonie sur Internet .Ils présentent tous les deux des approches différentes pour résoudre un même problème.

H323 est basé sur une approche traditionnelle du réseau à commutation de circuits. Quant à SIP, il est plus léger car basé sur une approche similaire au protocole http. Tous les deux utilisent le protocole RTP comme protocole de transfert des données multimédia. Au départ H323 fut conçu pour la téléphonie sur les réseaux sans QoS, mais on l'adopta pour qu'il prenne en considération l'évolution complexe de la téléphonie sur internet. Pour donner une idée de la complexité du protocole H323 par rapport à SIP, H323 est défini en un peu plus de 700 pages et SIP quand à lui en moins de 200 pages. La complexité de H323 provient encore du fait de la nécessité de faire appel à plusieurs protocoles simultanément pour établir un service, par contre SIP n'a pas ce problème.

SIP ne requiert pas de comptabilité descendante, SIP est un protocole horizontal au contraire de H323 : Les nouvelles versions de H323 doivent tenir compte des anciennes versions pour continuer à fonctionner. Ceci entraîne pour H323 de traîner un peu plus de codes pour chaque version. H323 ne reconnaît que les Codecs standardisés pour la transmission des données multimédias proprement dit alors que SIP, au contraire, peut très bien en reconnaître d'autres. Ainsi, on peut dire que SIP est plus évolutif que H323.

En résumé, La simplicité, la rapidité et la légèreté d'utilisation, tout en étant très complet, du protocole SIP sont autant d'arguments qui pourraient permettre à SIP de convaincre les investisseurs. De plus, ses avancées en matière de sécurité des messages sont un atout important par rapport à ses concurrents [09].

I.7 Protocoles de transport

I.7.1 Le protocole RTP

I.7.1.1 Description générale de RTP

RTP (Real time Transport Protocol), standardisé en 1996, est un protocole qui a été développé par l'IETF afin de faciliter le transport temps réel de bout en bout des flots données audio et vidéo sur les réseaux IP. L'utilisation de RTP se fait généralement au-dessus d'UDP ce qui permet d'atteindre plus facilement le temps réel. Les applications temps réels comme la parole numérique ou la visioconférence.

De plus RTP est un protocole qui se trouve dans un environnement multipoint, donc on peut dire que RTP possède à sa charge, la gestion du temps réel, mais aussi l'administration de la session multipoint.

I.7.1.2 Les fonctions de RTP

Le protocole RTP a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie.

RTP est un protocole de bout en bout, volontairement incomplet et malléable pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de l'application, Il est aussi un protocole adapté aux applications présentant des propriétés temps réel. Il permet ainsi de :

- Mettre en place une séquence des paquets par une numérotation et ce, afin de permettre ainsi la détection des paquets perdus, si les paquets ne sont pas perdus en trop grands nombres, cependant il est très important de savoir quel est le paquet qui a été perdu afin de pouvoir pallier à cette perte.
- Identifier le contenu des données pour leurs associer un transport sécurisé et reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur)
- L'identification de la source c'est à dire l'identification de l'expéditeur du paquet. Dans un multicast l'identité de la source doit être connue et déterminée.

• Transporter les applications audio et vidéo dans des trames qui sont incluses dans des paquets afin d'être transportées et doivent, de ce fait, être récupérées facilement au moment de la phase de segmentation des paquets afin que l'application soit décodée correctement.

I.7.1.3 Avantages et inconvénients

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo, etc.); de détecter les pertes de paquets; et d'identifier le contenu des paquets pour leur transmission sécurisée.

Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi il ne garantit pas le délai de livraison [10].

I.7.2 Le protocole RTCP

I.7.2.1 Description générale de RTCP

Le protocole RTCP est fondé sur la transmission périodique de paquets de contrôle à tous les participants d'une session. C'est le protocole UDP (par exemple) qui permet le multiplexage des paquets de données RTP et des paquets de contrôle RTCP.

Le protocole RTP utilise le protocole RTCP, Real-time Transport Control Protocol, qui transporte les informations supplémentaires suivantes pour la gestion de la session.

Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS.

Ces rapports comprennent le nombre de paquets perdus, ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir une QoS.

Parmi les principales fonctions qu'offre le protocole RTCP sont les suivants :

• Une synchronisation supplémentaire entre les médias : Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix, l'image ou même des applications numérisées sur plusieurs niveaux hiérarchiques peuvent voir les flots gérées et suivre des chemins différents.

- L'identification des participants à une session : en effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Le contrôle de la session : en effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations citées ci-dessus, Tandis que les paquets RTCP ne transportent en temps réel, que de la supervision. On peut détailler les paquets de supervision en 5 types:

- SR (Sender Report) : Ce rapport regroupe des statistiques concernant la transmission (pourcentage de perte, nombre cumulé de paquets perdus, variation de délai (gigue), etc.).
- RR (Receiver Report) : Ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.
- SDES (Source Description) : Carte de visite de la source (nom, e-mail, localisation).
- BYE : Message de fin de participation à une session.
- APP : Fonctions spécifiques à une application.

Le protocole de RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanant sur une session et ces participants. Par contre il fonctionne en stratégie bout à bout. Et il ne peut pas contrôler l'élément principal de la communication 'le réseau'[10].

I.8 Points forts et limites de la voix sur IP

Différentes sont les raisons qui peuvent pousser les entreprises à s'orienter vers la VoIP comme solution pour la téléphonie. Les avantages les plus marqués sont :

• **Réduction des coûts :** En effet le trafic véhiculé à travers le réseau RTC est plus couteux que sur un réseau IP. Réductions importantes pour des communications internationales en utilisant le VoIP, ces réductions deviennent encore plus intéressantes dans la mutualisation
voix/données du réseau IP intersites (WAN). Dans ce dernier cas, le gain est directement proportionnel au nombre de sites distants.

• **Standards ouverts :** La VoIP n'est plus uniquement H323, mais un usage multi protocoles selon les besoins de services nécessaires. Par exemple, H323 fonctionne en mode égale à égale alors que MGCP fonctionne en mode centralisé. Ces différences de conception offrent immédiatement une différence dans l'exploitation des terminaisons considérées.

• **Un réseau voix, vidéo et données (à la fois) :** Grace à l'intégration de la voix comme une application supplémentaire dans un réseau IP, ce dernier va simplifier la gestion des trois applications (voix, réseau et vidéo) par un seul transport IP. Une simplification de gestion mais également une mutualisation des efforts financiers vers un seul outil.

• **Un service PABX distribué ou centralisé :** Les PABX en réseau bénéficient de services centralisés tel que la messagerie vocale et la taxation. Cette même centralisation continue à être assurée sur un réseau VoIP sans limitation du nombre de canaux..L'utilisation de la VoIP met en commun un média qui peut à la fois offrir à un moment précis une bande passante maximum à la donnée, et dans une autre période une bande passante maximum à la voix, garantissant toujours la priorité à celle-ci.
Les points faibles de la voix sur IP sont :

• **Fiabilité et qualité sonore :** un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission qui n'est pas encore optimale. En effet, des désagréments tels la qualité de la reproduction de la voix du correspondant ainsi que le délai entre le moment où l'un des interlocuteurs parle et le moment où l'autre entend peuvent être extrêmement problématiques. De plus, il se peut que des morceaux de la conversation manquent (des paquets perdus pendant le transfert) sans être en mesure de savoir si des paquets ont été perdus et à quel moment.

• **Dépendance de l'infrastructure technologique et support administratif exigeant**

Les centres de relations IP peuvent être particulièrement vulnérables en cas d'improductivité de l'infrastructure. Par exemple, si la base de données n'est pas disponible, les centres ne peuvent tout simplement pas recevoir d'appels.

• **Vol :** les attaquants qui parviennent à accéder à un serveur VoIP peuvent également accéder aux messages vocaux stockés et au même au service téléphonique pour écouter des conversations ou effectuer des appels gratuits aux noms d'autres comptes.

• **Attaque de virus :** si un serveur VoIP est infecté par un virus, les utilisateurs risquent de ne plus pouvoir accéder au réseau téléphonique. Le virus peut également infecter d'autres ordinateurs connectés au système.

I.9 Discussion

Comme on a pu le voir tout au long de ce chapitre, la VoIP est la solution la plus rentable pour effectuer des conversations elle est devenue l'une des technologies en vogue en ce début de siècle suscite bien des intérêts venant en soutien aux autres technologies qui ont présentées des faiblesses.

La VoIP est une bonne solution en matière d'intégration, fiabilité et de coût. C'est la transmission de la voix sur un réseau IP.

Les constructeurs de l'ère se sont alors investis à la création de PBX pour gérer les paquets IP en fonction des différentes contraintes.

Chapitre II

Vulnérabilités et attaques contre la VoIP

II.1 Préambule

Si aujourd'hui, la technologie VoIP fait partie intégrante des offres d'accès Internet à haut débit. Le succès de cette technologie s'explique également par les appels gratuits entre les utilisateurs de VoIP d'un même fournisseur et les offres bon marché et tout compris pour l'interface vers les systèmes de téléphonie classique.

En plus d'une telle déficience organisationnelle, il existe un grand nombre d'attaques dirigées contre les infrastructures techniques. Avant de les aborder, il est essentiel de bien comprendre le fonctionnement de base de la sécurité sur le protocole SIP. Nous nous concentrerons sur le protocole SIP, dans la mesure où le développement se dirige clairement du protocole H.323 vers le SIP.

Mais il ne s'agit pas non plus d'évoquer les tâches réalisables grâce au protocole.
Durant ce chapitre on va montrer les vulnérabilités de la voix sur IP et démontrer comment des attaques peuvent être menées contre la technologie VoIP .

Les attaques décrites dans ce chapitre proviennent d'un environnement VoIP couramment utilisé, dont le protocole de signalisation est le SIP. Par ailleurs, les attaques sont basées sur des méthodes elles aussi couramment utilisées.

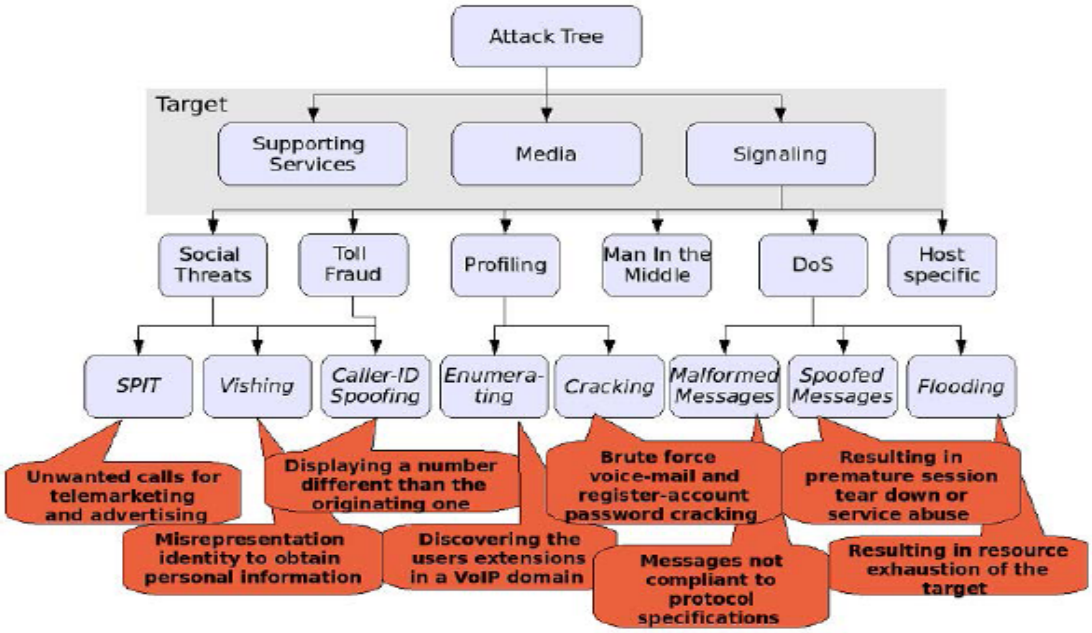


Figure II.1 Classification des attaques par protocole cible

II.2 Les vulnérabilités de l'infrastructure

Une infrastructure VoIP est composée de téléphones IP, Gateway, serveurs (proxy, register, etc.) Chaque élément, que ce soit un système embarqué ou un serveur standard tournant sur un système d'exploitation, est accessible via le réseau comme n'importe quel ordinateur.

Chacun comporte un processeur qui exécute des logiciels qui peuvent être attaqués ou employés en tant que points de lancement d'une attaque plus profonde.

II.2.1 Faiblesses dans la configuration des dispositifs de la VoIP

Plusieurs dispositifs de la VoIP, dans leur configuration par défaut, peuvent avoir une variété de ports TCP et UDP ouverts. Les services fonctionnant sur ces ports peuvent être vulnérables aux attaques DoS ou buffer overflow.

Plusieurs dispositifs de la VoIP exécutent également un serveur WEB pour la gestion à distance qui peut être vulnérable aux attaques buffer overflow et à la divulgation d'informations [02].

Si les services accessibles ne sont pas configurés avec un mot de passe, un attaquant peut acquérir un accès non autorisé à ce dispositif.
Les services SNMP (Simple Network Management Protocol) offerts par ces dispositifs peuvent être vulnérables aux attaques de reconnaissance ou attaques d'overflow.
Plusieurs dispositifs de la VoIP sont configurés pour télécharger périodiquement un fichier de configuration depuis un serveur par TFTP ou d'autres mécanismes. Un attaquant peut potentiellement détourner ou mystifier cette connexion et tromper le dispositif qui va télécharger un fichier de configuration malveillant à la place du véritable fichier.

II.2.2 Les téléphones IP

Un pirate peut compromettre un dispositif de téléphonie sur IP, par exemple un téléphone IP, un softphone et autres programmes ou matériels clients. Généralement, il obtient les privilèges qui lui permettent de commander complètement la fonctionnalité du dispositif.

Compromettre un point final (téléphone IP) peut être fait à distance ou par un accès physique au dispositif. Le pirate pourrait modifier les aspects opérationnels d'un tel dispositif:
La pile du système d'exploitation peut être changée. Ainsi la présence de l'attaquant ne sera pas remarquée.

Aussi un firmware modifié de manière malveillante peut être téléchargé et installé. Les modifications faites à la configuration des logiciels de téléphonie IP peuvent permettre:

- Aux appels entrants d'être réorientés vers un autre point final sans que l'utilisateur soit au courant.
- Aux appels d'être surveillés.
- A l'information de la signalisation et/ou les paquets contenant de la voix d'être routés vers un autre dispositif et également d'être enregistrés et/ou modifiés.

De compromettre la disponibilité du point final. Par exemple, ce dernier peut rejeter automatiquement toutes les requêtes d'appel, ou encore, éliminer tout déclenchement de notification tel qu'un son, une notification visuelle à l'arrivée d'un appel. Les appels peuvent également être interrompus à l'improviste (quelques téléphones IP permettent ceci via une interface web).

D'autres conséquences possibles sont:

- Des backdoors pourraient été installés.
- Toutes les informations concernant l'utilisateur qui sont stockées sur le dispositif pourraient été extraites.

L'acquisition d'un accès non autorisé sur un dispositif de téléphonie IP peut être le résultat d'un autre élément compromis sur le réseau IP, ou de l'information récoltée sur le réseau.

Les softphones ne réagissent pas de la même façon aux attaques comparés à leur homologues téléphones IP. Ils sont plus susceptibles aux attaques dues au nombre de vecteurs inclus dans le système, à savoir les vulnérabilités du système d'exploitation, les vulnérabilités de l'application, les vulnérabilités du service, des vers, des virus, etc. En plus, le softphone demeure sur le segment de données, est ainsi sensible aux attaques lancées contre ce segment et pas simplement contre l'hôte qui héberge l'application softphone.

Les téléphones IP exécutent quant à eux leurs propres systèmes d'exploitation avec un nombre limité de services supportés et possèdent donc moins de vulnérabilités.

II.2.3 Les serveurs

Un pirate peut viser les serveurs qui fournissent le réseau de téléphonie sur IP.

Compromettre une telle entité mettra généralement en péril tout le réseau de téléphonie dont le serveur fait partie.

Par exemple, si un serveur de signalisation est compromis, un attaquant peut contrôler totalement l'information de signalisation pour différents appels. Ces informations sont routées à travers le serveur compromis. Avoir le contrôle de l'information de signalisation permet à un attaquant de changer n'importe quel paramètre relatif à l'appel.

Si un serveur de téléphonie IP est installé sur un système d'exploitation, il peut être une cible pour les virus, les vers, ou n'importe quel code malveillant.

II.2.4 Les vulnérabilités du système d'exploitation

Ces vulnérabilités sont pour la plupart relatives au manque de sécurité lors de la phase initiale de développement du système d'exploitation et ne sont découvertes qu'après le lancement du produit.

Une des principales vulnérabilités des systèmes d'exploitation est le buffer overflow. Il permet à un attaquant de prendre le contrôle partiel ou complet de la machine.

Les dispositifs de la VoIP tels que les téléphones IP, Call Managers, Gateway et les serveurs proxy, héritent les mêmes vulnérabilités du système d'exploitation ou du firmware sur lequel ils tournent.

Il existe une centaine de vulnérabilités exploitables à distance sur Windows et même sur Linux. Un grand nombre de ces exploits sont disponibles librement et prêts à être téléchargés sur l'Internet.

Peu importe comment, une application de la VoIP s'avère être sûre, celle-ci devient menacé si le système d'exploitation sur lequel elle tourne est compromis [02].

II.3. Attaques de sécurité les plus répandus :

II.3.1 Attaques contre les protocoles de signalisation

La signalisation est la phase la plus importante de toute interaction de télécommunication.

Elle est la cible principale d'un large éventail d'attaques de sécurité. L'objectif de l'attaque consiste à empêcher les utilisateurs légitimes d'exploiter l'équipement ou l'infrastructure attaqué [15].

Méthode	Descriptif
REGISTER	Avec cette méthode, un client peut s'inscrire ou annuler son inscription d'un serveur mandataire. Il est donc prêt et disponible pour la communication VoIP. Pour annuler l'inscription, la valeur pour la période est réglée sur 0.
INVITE	Il s'agit de la méthode la plus importante. Sans elle, vous n'auriez pas besoin du protocole SIP. Toutes les méthodes de traçage lui sont subordonnées, même si elles sont toutes utilisées seules.
ACK	Si un appel (par exemple une vidéo conférence) est paramétré, c'est une requête ACK indépendante qui en prend connaissance au final. Juste après la requête ACK, la connexion en continu est paramétrée.
BYE	Ce message a pour but de terminer un appel de manière régulière. Grâce à ce message, il devient possible de mettre fin à une transaction établie au moyen de la méthode INVITE. Un message BYE est traité au moyen du paramètre du dialogue approprié (Call-ID ou balise).
CANCEL	Avec CANCEL, une connexion établie peut être interrompue avant que l'appel ne soit établi. Cette méthode est également utilisée dans des situations d'erreurs.
OPTIONS	Cette méthode de requête est utilisée afin d'échanger les méthodes de requêtes supportées ou les attributs des médias pour la transmission.
NOTIFY	Méthode de requête supplémentaire définie dans le document RFC 3265. Elle permet d'échanger les messages de statut d'une ressource vers laquelle un client est connecté. Par exemple, le client peut recevoir une indication d'arrivée de nouveaux messages vocaux.

Tableau I.1 : Méthodes des en-têtes de requêtes SIP

II.3.1.1 Attaques SIP/ARP dirigées contre VoIP

Un réseau exploité par de nombreux utilisateurs et un grand nombre d'applications différentes. Ce qui permet bien sûr à une personne malveillante de s'introduire plus facilement dans la communication, au moyen des systèmes informatiques.
Aspirer des appels téléphoniques et les rediffuser devant les partenaires de communication est sans aucun doute l'une des attaques sur VoIP les plus impressionnantes.

Comme mentionné, la signalisation est réalisée au moyen d'un serveur mandataire SIP, et la communication entre plusieurs partenaires est elle-même possible grâce à la technique *peer-to-peer*.

Dans cet exemple, vous souhaitez écouter l'appel entre Sid Ali et Yazid.
Pour ce faire, vous devez lancer ce qu'on appelle en anglais une attaque *man-in-the-middle* au moyen d'un empoisonnement ARP dans le but de convaincre à la fois le serveur mandataire et les téléphones VoIP de Sid Ali et de Yazid qu'ils veulent communiquer avec vous et non entre eux.

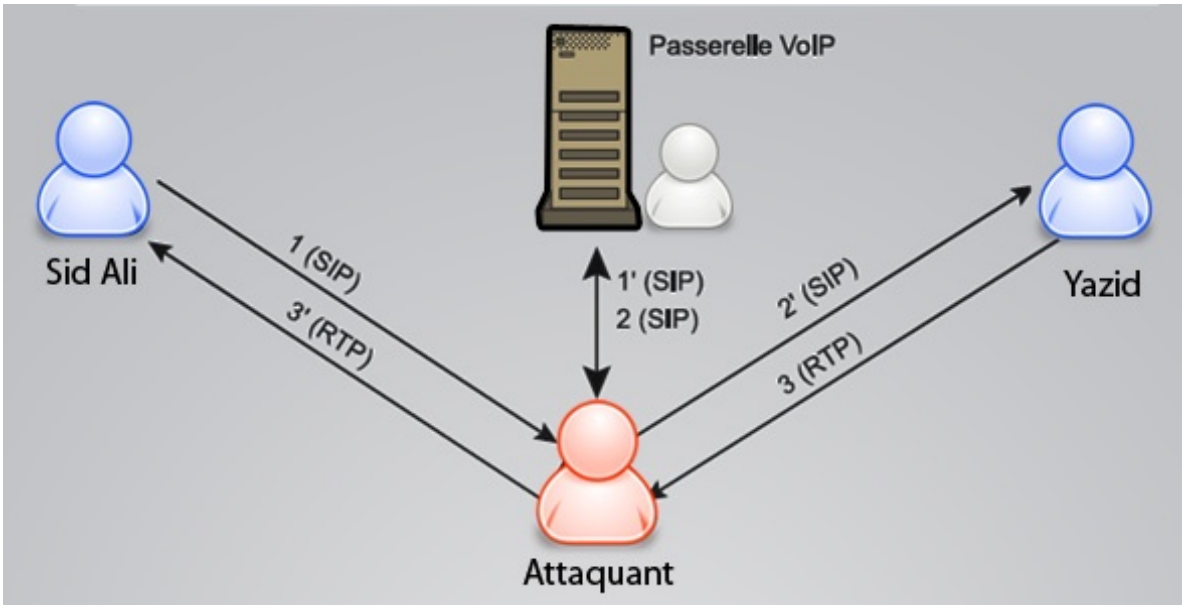


Figure II.2. Aspiration d'une transmission VoIP

Vous trouverez dans la Figure II.2 un plan illustrant l'aspiration d'une transmission VoIP. Tout d'abord, l'appel est paramétré. Sid Ali envoie la requête pour appeler Yazid au serveur mandataire SIP. Ce message est intercepté puis transmis à la personne malveillante. Le serveur mandataire SIP tente désormais de joindre Yazid pour lui indiquer que Sid Ali souhaite l'appeler. Ce message est également intercepté puis transmis à la personne malveillante.

Après une initialisation de l'appel réussie, l'appel actuel (qui a recours au protocole RTP) entre Sid Ali et Yazid commence. Cette communication RTP est également interceptée puis transmise par la personne malveillante [15].

II.3.1.2 Attaques de déni de service (DoS)

Cette attaque a pour objectif de réaliser des dégâts (arrêt temporaire, dysfonctionnement des appels) aux réseaux VoIP. Nous trouvons trois catégories d'attaques par inondation de messages SIP.

La première catégorie consiste en l'inondation par des messages SIP corrects, il s'agit d'envoyer un nombre important de messages SIP comme SIP INVITE pour réaliser un déni de services contre un terminal ou un proxy SIP.

La deuxième catégorie consiste en l'inondation par des messages malformés pour faire tomber des serveurs et la troisième consiste à envoyer des messages malformés exploitant des vulnérabilités bien spécifiques. Nous trouvons aussi l'envoi massif de messages SIP INVITE avec un champ REQUEST URI valide. Dans ce cas de figure, l'attaquant appelle un téléphone SIP enregistré auprès du proxy SIP qui le surcharge par des messages SIP INVITE.

Par conséquent, le serveur proxy va réserver des ressources de mémoire pour ces appels ce qui génère un débordement de mémoire auprès du serveur.

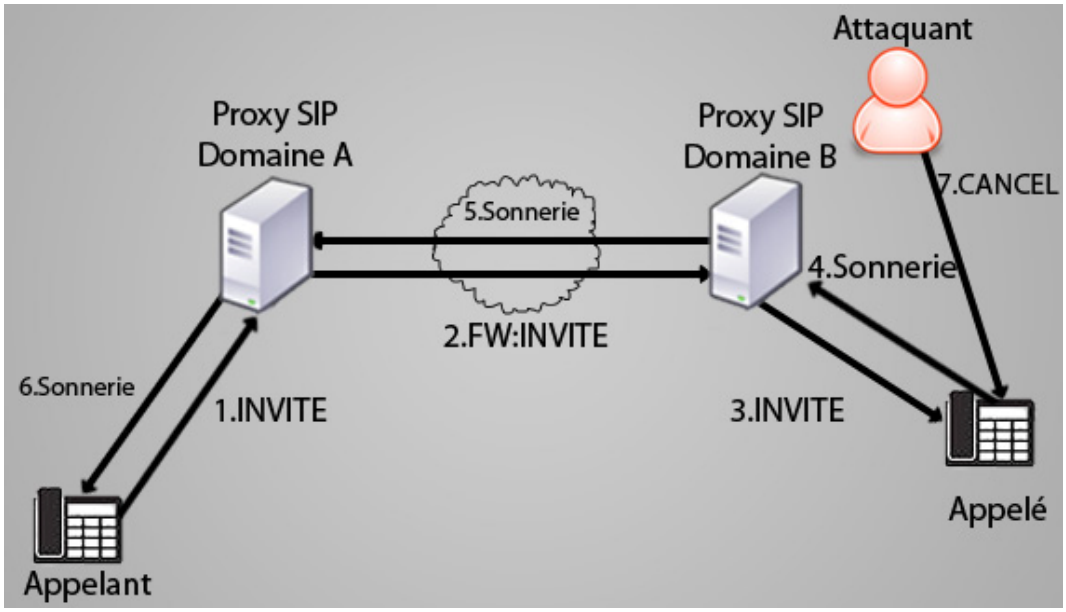


Figure II.3 : Attaque DoS via une requête CANCEL

II.3.1.3 Attaque d'usurpation d'identité

Elle s'appuie sur le vol d'identité et du mot de passe d'un client SIP par l'écoute du trafic SIP ou sur l'acquisition via une autre voie du couple (nom d'utilisateur et mot de passe) et les utilise pour avoir un accès non autorisé . Le vol d'identité peut se faire par une attaque de type man-in-the-middle ; l'utilisateur SIP entre ses coordonnées d'authentification et l'attaquant suit l'échange du trafic entre le client et le serveur et récupère les coordonnées d'un utilisateur SIP pour les utiliser ultérieurement. Sur la figure II.4, nous présentons une attaque d'usurpation d'identité dans le cas du réseau P2PSIP. L'attaquant utilise le nom d'utilisateur de la victime pour modifier la correspondance entre l'adresse logique (de la victime) et son adresse physique.

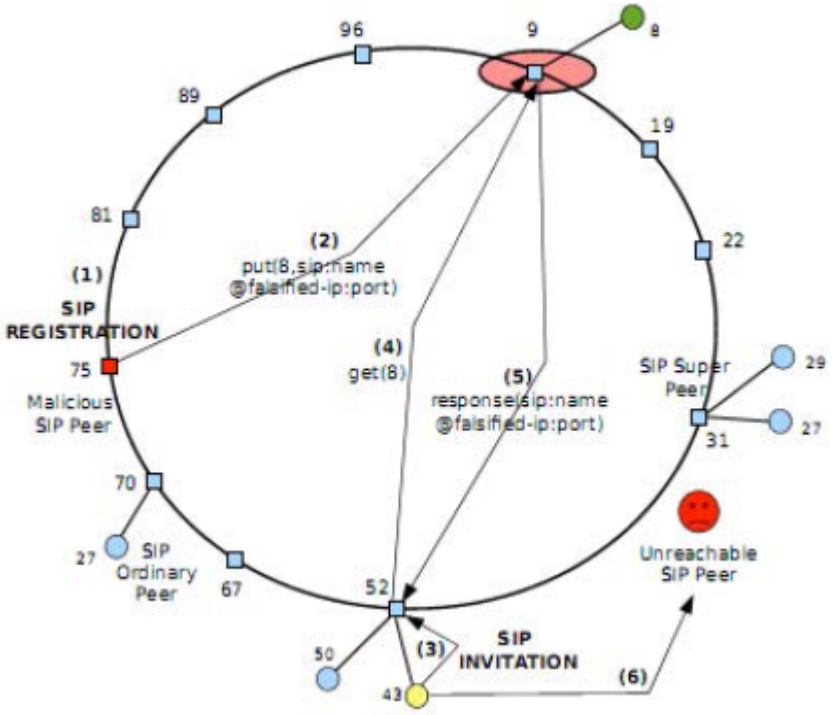


Figure II.4 : Exemple d'une attaque d'usurpation d'identité en P2PSIP

Un pair malveillant envoie un message P2P PUT avec une nouvelle adresse physique. Ainsi, quand un utilisateur P2PSIP cherche à contacter la victime, il va chercher son entrée dans la DHT et tombe sur une adresse physique inexistante. Cette attaque simple permet de rendre les paires victimes injoignables [02].

II.3.1.4 Attaques par messages malformés

L'attaque par messages malformés consiste à construire et envoyer des messages SIP malformés d'une façon aléatoire ou semi aléatoire.

Cette technique de génération de trafic s'appelle le fuzzing. Bien que le proxy SIP possède la capacité de corriger des requêtes SIP et de modifier les différents champs, ceci n'arrête pas les attaques dues aux messages malformés. Elles peuvent engendrer l'arrêt brutal des services VoIP après avoir causé des dégâts comme l'effondrement du système par une attaque du débordement de mémoire (bu_erover_ow) par exemple.

L'attaquant peut aussi obtenir un accès non autorisé au système et même injecter un code pour l'exécuter à distance [16].

II.3.1.5 Attaque SPIT (Spam over IP Telephone)

L'attaque appelée SPIT est l'un des dangers les plus fréquemment mentionnés en cas d'installation de la technologie VoIP. Cette attaque consiste à envoyer des messages vocaux de la même façon que les publicités e-mail non désirées ou spam.
Contrairement aux appels automatisés dans le monde des services téléphoniques ordinaires, les appels VoIP ne génèrent pas de coûts dès le début. A l'instar des spams traditionnels bien connus, le *spitter* utilise l'adresse d'une victime, dans ce cas, il ne s'agit pas de son adresse e-mail, mais de son adresse SIP.

Avec le succès que rencontre la téléphonie IP, ce n'est qu'une question de temps pour obtenir facilement de nombreuses adresses SIP valides, surtout si les livres d'adresses centrales vont être réellement utilisés.

Le spitter appelle un numéro SIP trouvé, le serveur mandataire SIP de la victime va traiter cet appel et la victime elle-même n'a d'autre choix que d'écouter le message spam élaborée par le spitter sur par exemple la virilité de quelqu'un. Tout comme les spammers, le spitter n'a besoin que d'un seul élément, le débit. En effet, les messages vocaux consomment bien plus de ressources que les e-mails. Un message de 15 secondes par exemple (aucune victime ne supporterait un message plus long) équivaut à 120 Ko au moyen d'un codec de 64 Kbps. En ayant recours à des chevaux de Troie, encore une fois comme les spams, un utilisateur
Internet non protégé pourrait être induit à envoyer une attaque SPIT au travers de sa bande passante [14].

II.3.1.6 Attaque de l'homme du milieu

Dans le cas où il n'y a pas des mécanismes d'authentification forte, de nombreuses situations permettent à un attaquant de se positionner entre un appelant et l'appelé. SIP met en œuvre un schéma d'authentification similaire à HTTP.

Tous les serveurs SIP comme le proxy et le serveur de redirection peuvent authentifier un client SIP UAC par un défi cryptographique basé sur le secret partagé (généralement le mot de passe stocké dans le serveur). Cette authentification est généralement faite dans un seul sens, du client vers le serveur.

L'attaque de l'homme du milieu peut être établie par le scénario décrit sur la figure II.5. Le client SIP envoie un message INVITE à son serveur proxy SIP, l'attaquant Charlie intercepte le message et envoie une réponse de redirection forgée à mené vers son adresse physique. Comme il n'a pas authentifié le serveur proxy, le client SIP accepte la réponse et redirige l'appel vers l'attaquant.

Le vrai proxy SIP peut être neutralisé par un déni de service ou en exploitant une situation de concurrence.

En même temps, l'attaquant remplace l'emplacement de l'émetteur par son adresse IP dans le champ Contact (ce champ indique l'adresse physique de l'appelé). L'attaquant peut aussi exploiter les champs via et REQUEST-URI dans les messages SIP afin de modifier l'itinéraire des requêtes SIP. Ensuite, il envoie le message falsifié vers l'appelé Alice. Ainsi, tous les messages de signalisation communiqués entre l'appelé et l'appelant passeront dorénavant par l'attaquant.

Le vol de la session de signalisation entre les deux clients est une première étape vers le vol de la session d'échange de média [16].

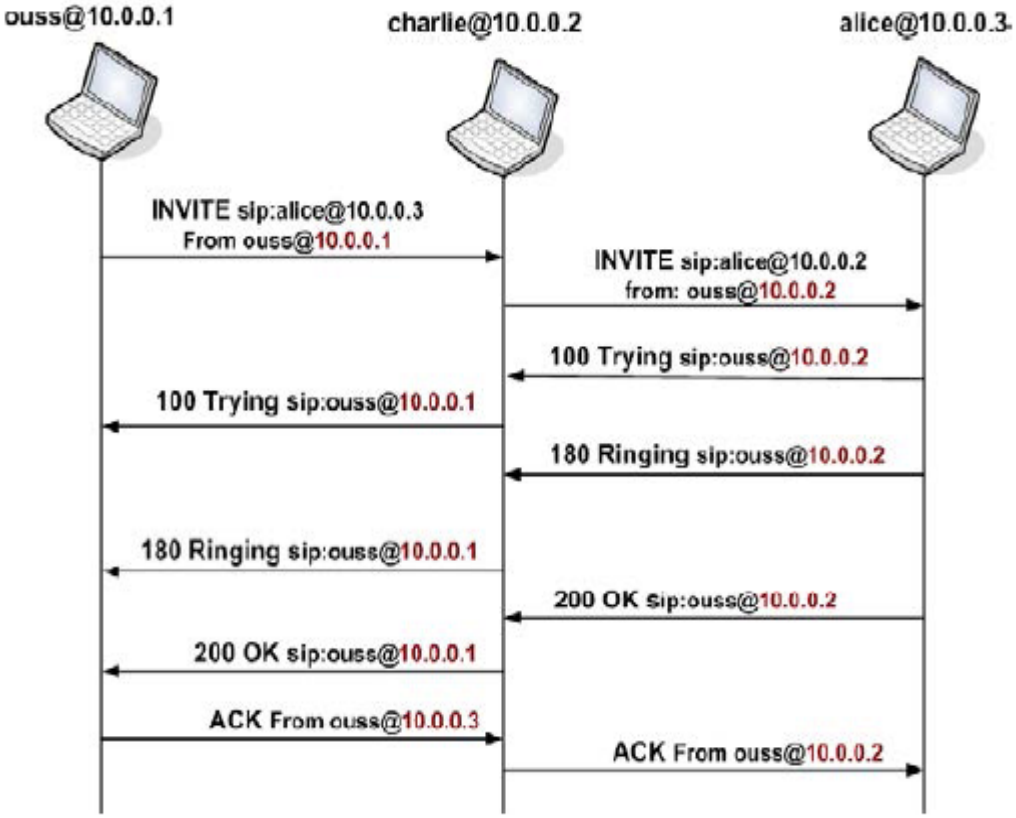


Figure II.5 Attaque de l'homme du milieu

II.3.1.7 Détournement d'un enregistrement

Le processus d'enregistrement dans le réseau VoIP SIP utilise le protocole UDP pour transporter les messages ce qui simplifie la génération des messages usurpés. Le serveur d'enregistrement n'applique pas de règles fortes pour protéger les clients enregistrés. Quand l'authentification est imposée, elle peut inclure un identifiant MD5 pour le nom d'utilisateur, un mot de passe et une estampille temporelle. Cette attaque a pour but le détournement des appels vers l'attaquant ou vers une destination SIP inexistante (voir figure II.4). L'attaquant réalise cette attaque par étapes, la première consiste à obtenir un carnet d'adresses enregistrées auprès du serveur registrar, il peut l'avoir en scannant le réseau et en cherchant des adresses SIP URI. Il peut aussi envoyer des messages SIP OPTIONS et SIP INVITE pour vérifier si une adresse SIP est valide ou pas. La deuxième étape consiste à s'authentifier auprès du serveur, cette

opération est faite généralement soit par une attaque de fraude ou par une attaque de dictionnaire.

II.3.2Attaques contre les protocoles médias

Dans cette section, nous nous intéressons aux attaques de protocoles médias RTP et RTCP. Les attaques présentées sont le DoS, l'écoute du média et les attaques de manipulation du trafic.

II.3.2.1 Écoute et analyse du trafic

Ceci regroupe l'ensemble des tentatives de collecte des informations sensibles concernant le média pour préparer une attaque plus développée ou pour avoir plus de connaissance sur les parties communicantes ou sur l'entreprise.

Cette attaque donne la possibilité à l'attaquant d'avoir le contrôle sur l'échange de messages RTP non protégés entre clients VoIP. Cette catégorie d'attaques inclut l'analyse du trafic qui peut être active ou passive comme la collecte, l'analyse et le décodage des messages RTP. Cette attaque a pour objectif d'extraire des informations textuelles ou verbales comme les numéros de carte de crédit ou d'analyser les communications pour établir des modèles de communications que l'attaquant peut utiliser ultérieurement.

La qualité de service est essentielle dans le service VoIP. Si un attaquant réussit à dégrader la qualité de service comme la disponibilité ou la gigue, la communication SIP devient incompréhensible.

Par conséquent, il suffit que l'attaquant encombre un proxy SIP, un routeur ou une passerelle média par des messages RTP malveillants pour qu'il dégrade la qualité des services VoIP. L'attaquant peut aussi injecter des messages RTP (des messages vocaux) pour qu'ils perturbent les parties communicantes. Cette attaque se fait par étape : initialement, l'attaquant doit savoir qu'il y a une session établie entre deux clients SIP. Ensuite, il prépare des messages RTP usurpés par l'identité d'un des deux clients, et il les envoie massivement vers l'autre. Comme la signalisation et l'échange

des messages média sont séparés par la définition du trapézoïde SIP, le protocole de signalisation n'a aucun contrôle sur la qualité de service du transfert du média et sur le chemin pris par les messages.

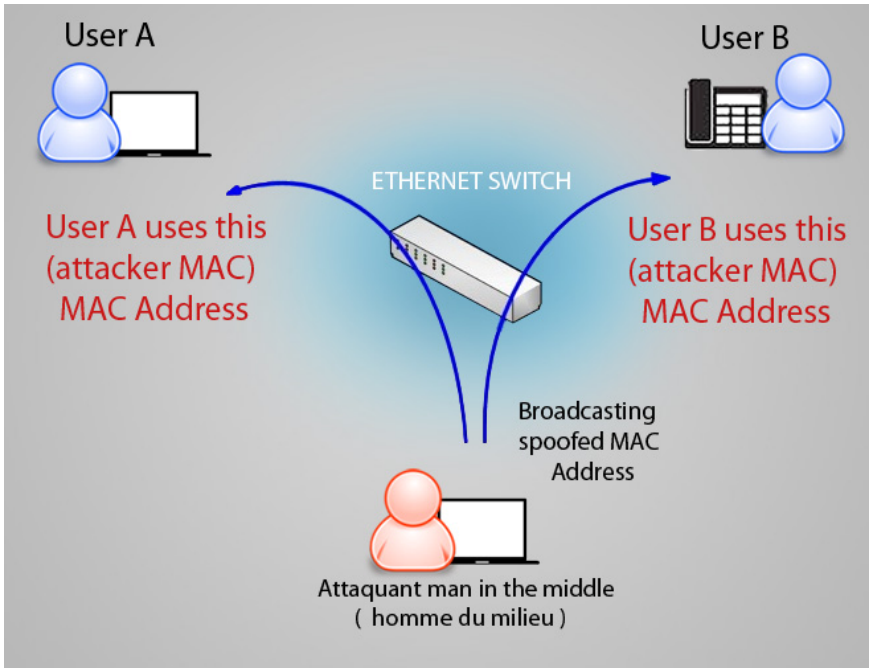


Figure II.6 : Exemple de détournement d'appel " Man in the middle "

II.3.2.2 Attaques par manipulation de messages RTCP

L'attaquant peut perturber le fonctionnement du protocole RTCP. Ce protocole est responsable des rapports et des statistiques concernant le trafic RTP. En écoutant et analysant le trafic, l'attaquant intercepte les rapports RTCP comme le rapport de l'appelant et le rapport de l'appelé. Ensuite, il modifie le contenu et les paramètres dans ces rapports pour envoyer des fausses informations sur les échanges RTP. Par exemple, l'attaquant peut envoyer des rapports indiquant qu'il n'y a pas de perte de messages durant la conversation audio, ce qui mène à des pertes de messages plus grandes et par conséquent rend la communication incompréhensible.

II.3.3 Attaques contre les services support

Les services support jouent un rôle important dans la continuité opérationnelle et le fonctionnement des services VoIP. Nous y trouvons des services comme le DNS qui permet au serveur proxy de résoudre les noms de domaine, le service DHCP qui affecte les adresses de contact au client et d'autres services comme le transfert des fichiers pour la configuration par exemple. Parmi les services support critiques, nous trouvons le système de facturation qui représente, s'il a des dysfonctionnements, une menace financière pour le fournisseur. Nous détaillons dans cette section les plus importantes attaques contre ses services.

II.3.3.1 Attaques contre le système de paiement

La facturation est un service fondamental pour tous les services VoIP commerciaux et il a un impact direct sur chaque client VoIP.

L'une des exigences les plus importantes de facturation est qu'elle doit être sécurisée et qu'elle représente un service fiable. Du côté client VoIP, la facturation ne doit que lui faire payer les appels qu'il a vraiment passé et pour la durée consommée.

Les systèmes de facturation existants sont basés sur la signalisation VoIP. Dans le cas du protocole SIP, elle commence à partir de la réception du message SIP 200 OK; ce message valide que l'appelé a accepté l'appel. Ainsi, toute vulnérabilité dans le système de signalisation est une vulnérabilité potentielle de la facturation VoIP. Un attaquant peut intercepter l'établissement.

II.3.3.2 Attaque de l'accès non autorisé

Cette attaque consiste à accéder à un service, une fonctionnalité, ou un élément de réseau sans autorisation appropriée.
Les attaques de cette catégorie peuvent être utilisées pour soutenir d'autres attaques, y compris des attaques de déni de service, la fraude et même l'usurpation d'identité parce

que l'attaquant peut prendre le contrôle d'un équipement, d'une ressource, ou de l'accès à un réseau. La différence entre l'accès non autorisé et le masquage, c'est que l'attaquant dans le premier cas a le contrôle d'une ressource ou l'accès au réseau en exploitant une vulnérabilité comme le dépassement de mémoire, la configuration par défaut ou la signalisation non sécurisée. Par exemple, un attaquant qui contrôle un proxy SIP où il a un accès administratif peut interrompre le service de signalisation par la suppression des fichiers systèmes.

II.3.3.3 Ingénierie sociale

L'ingénierie sociale est la capacité d'abuser ou de profiter des services VoIP pour un gain personnel ou financier. Cette catégorie d'attaques est l'une des plus critiques pour les opérateurs de télécommunications et les fournisseurs de VoIP. L'ingénierie sociale est une préoccupation importante en matière de sécurité et de confidentialité.

Différentes attaques sont comprises dans cette classe comme la déclaration des informations fausses délivrées expressément dans le but de tromper ou utiliser une fausse déclaration. Nous trouvons aussi la présentation préméditée d'une fausse identité montrant des informations de quelqu'un d'autre afin de contourner les mécanismes d'authentification.
Cette catégorie inclut le vol de services qui consiste à gagner illégalement des revenus provenant des services de quelqu'un d'autre, par exemple la facturation des appels VoIP [16].

II.4. Discussion

Il est évident que la technologie VoIP est l'une des techniques de ces dernières années parmi les plus prometteuses et est en passe de devenir une nouvelle application phare d'Internet. C’est pourquoi, elle est de plus en plus ciblée par des attaques et il en existe plusieurs. Durant ce chapitre, nous avons cité quelques unes qui sont les plus courantes et utilisées dans les réseaux VoIP.

Pour se protéger au mieux de ces attaques, nous devons installer un réseau bien sécurisé. Ce que nous ferons au dernier chapitre, qui consiste à mettre en place une bonne pratique de sécurisation.

Chapitre III

Mise en place de la solution VoIP basée sur Asterisk

III.1 Préambule

Apres avoir pris connaissance de la voix sur IP, ça vulnérabilité ainsi que les attaques possibles, nous allons vous présenter durant ce chapitre un outil très populaire de la VoIP qui est Asterisk.

On montrera les étapes de son installation et de sa configuration sous le système d'exploitation Linux, ainsi que l'installation et la configuration de X-Lite qui est un téléphone VoIP softphone, freeware, puis nous terminerons avec un appel test entre deux clients X-Lite.

III.2 Présentation d'Asterisk

Asterisk est un autocommutateur téléphonique privée (PABX) open source pour les systèmes d'exploitation UNIX, il est publié sous licence GPL.

Il comprend un nombre très élevé de fonctions, tel que les appels téléphoniques, la messagerie vocale, les files d'attentes, les conférences, etc. Il implémente plusieurs protocoles H.320, H.323, SIP, IAX, MGCP, SCCP et UNISTIM [04].

Certaines sociétés dont Digium éditent maintenant des distributions entièrement consacrée à Asterisk parmi lesquelles on peut citer :

- Asterisk Now (édité par Digium)
- Trixbox (anciennement Asterisk@home)
- Xivo (édité par Avencall, société française et basée sur Debian)

III.2.1 Historique

Asterisk est né en 1999, créé par un étudiant de l'université d'Auburn (États-Unis - Alabama). À la recherche d'un commutateur téléphonique privé pour créer un centre de support technique sur Linux, il est dissuadé par les tarifs trop élevés des solutions existantes, et décide de se créer son propre routeur d'appels sous Linux .

Le PBX open source Asterisk a vu le jour quand Mark Spencer, a voulu acquérir un PBX traditionnel pour sa société. Le créateur d'Asterisk, trouvant que le prix d'acquisition d'un PBX traditionnel était démesuré, initia un projet open source. Il a donc commencé à développer Asterisk.

Les programmeurs Open Source du monde entier ont contribué à l'écriture du source, aux expérimentations, et aux patches correctifs des bugs en provenance de la communauté ont apporté une aide précieuse au développement de ce logiciel [01].

III.2.2 Architecture

Asterisk est soigneusement conçu pour une flexibilité maximale. Les APIs spécifiques sont définies autour d'un système PBX central. Ce noyau avancé manipule l'interconnexion interne du PBX proprement soustrait des protocoles spécifiques des codecs et des interfaces matérielles des applications de téléphonie. Cela permet à Asterisk d'utiliser n'importe quel matériel approprié et technologie disponible (maintenant ou à l'avenir) pour exécuter ces fonctions essentielles, en connectant le matériel et les applications [12].

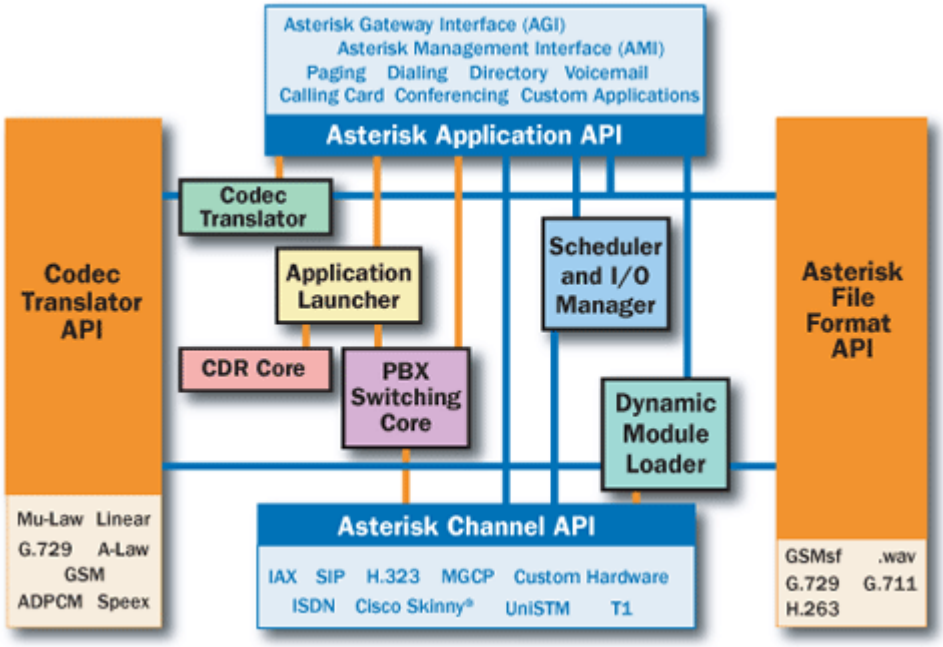


Figure III.1 Architecture D'asterisk

III.2.3 Fonctionnalités :

Asterisk satisfait de nombreux types de besoins, il est également utilisé dans un cadre professionnel, en tant que commutateur téléphonique d'entreprise, de passerelle vers le réseau téléphonique, de serveur de messagerie vocale ou de serveur d'audioconférence. Une des grandes forces d'Asterisk et des logiciels libres de télécommunication en général, tient dans ce caractère multifonctionnel. En effet, les fonctions mentionnées ci-dessus peuvent être assurées soit sur un système unique, par exemple pour réduire le coût d'installation, soit sur différents systèmes hébergeant chacun une instance d'Asterisk, afin d'améliorer la disponibilité d'ensemble des différents composants du service téléphonique.

Asterisk offre les fonctionnalités suivantes :

- Messagerie vocale
- Conférence téléphonique
- Répondeur vocal interactif
- Mise en attente d'appels
- Services d'identification de l'appelant
- VoIP

III.3 Principales fonctions :

- **PBX Switching Core :** Système de commutation de central téléphonique privé, reliant ensemble les appels entre divers utilisateurs et des tâches automatisées. Le noyau de commutation relie d'une manière transparente des appels arrivant sur divers interfaces de matériel et de logiciel.

- **Application Launcher :** Lance les applications qui assurent des services pour des usagers, tels que la messagerie vocale, la lecture de messages et le listage de répertoires.

- **Codec Translator :** Utilise des modules de codec pour le codage et le décodage de divers formats de compression audio utilisés dans l'industrie de la téléphonie. Un certain nombre de codecs sont disponibles pour pallier aux divers besoins et pour arriver au meilleur équilibre entre la qualité audio et l'utilisation de la bande passante.

- **Scheduler & I/O Manager :** Ils traitent la planification des tâches de bas niveau et la gestion du système pour une performance optimale dans toutes les conditions de charge [01].

III.4 Les APIs

Asterisk Application API : Elle autorise différents modules de tâches à être lancé pour exécuter diverses fonctions.

Communication, audioconférence, pagination, liste d'annuaire, messagerie vocale, transmission de données intégrée, et n'importe quelle autre tâche qu'un système PBX standard exécute actuellement ou exécuterait dans l'avenir, sont mises en œuvre par ces modules distincts.

- **Asterisk Translator API :** Charge les modules de codec pour supporter divers formats de codage et de décodage audio tels que le GSM, la Mu-Law, l'A-Law, et même le MP3.

- **Asterisk Channel API :** Cette API gère le type de raccordement sur lequel arrive un appelant, que ce soit une connexion VoIP, un RNIS, un PRI, une signalisation de bit dérobé, ou une autre technologie. Des modules dynamiques sont chargés pour gérer les détails de la couche basse de ces connexions.

- **Asterisk File Format API :** Elle permet la lecture et l'écriture de divers formats de fichiers pour le stockage de données dans le file system.

Sa particularité modulaire permet à Asterisk d'intégrer de façon continue le matériel de commutation téléphonique actuellement mise en œuvre, et les technologies de Voix par paquet en constante augmentation, émergeant aujourd'hui.

La capacité de charger des modules de codec permet à Asterisk d'être compatible avec le codec extrêmement compact nécessaire à la Voix sur IP sur des connexions lentes comme un modem téléphonique tout en maintenant une haute qualité audio sur des types de connexion moins "étroites" [01].

III.5 Architecture du réseau VoIP déployé

La figure III.2 montre l'architecture adoptée au cours de la configuration de la solution de VoIP à base d'Asterisk

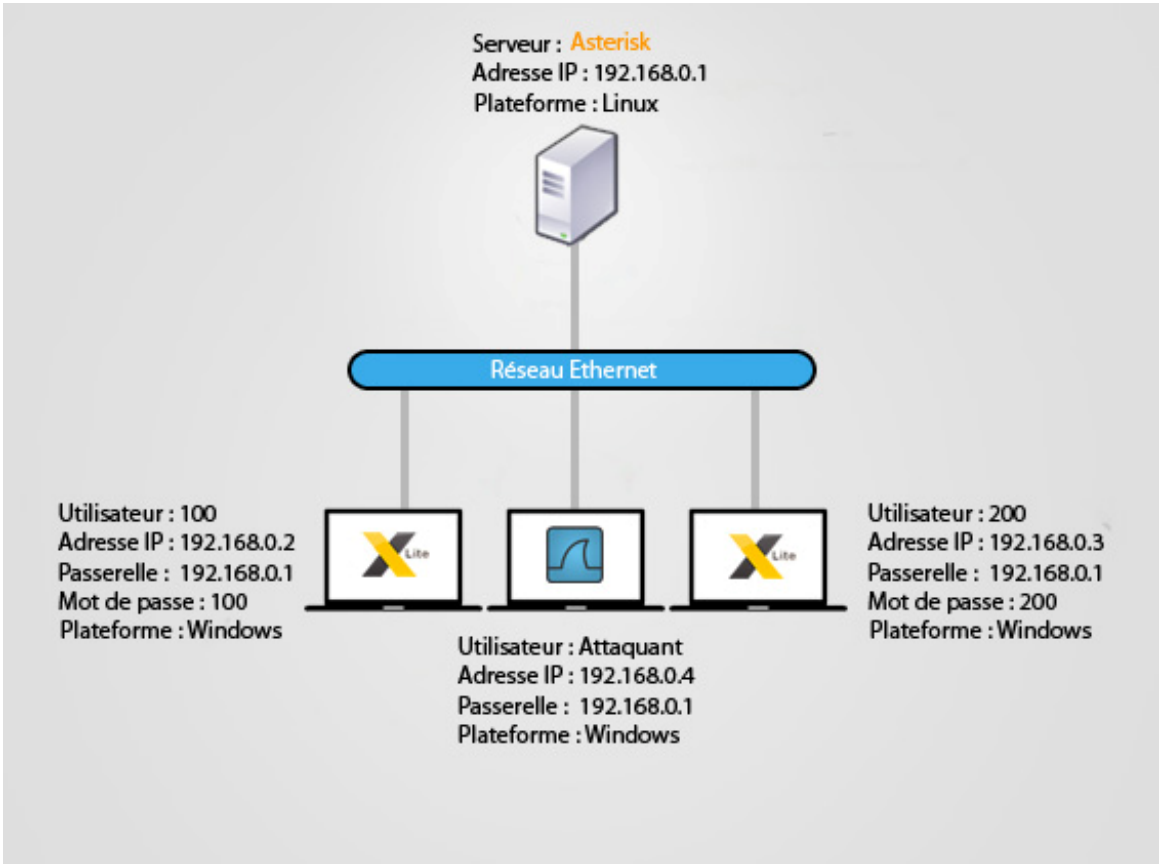


Figure III.2 : Architecture du réseau VoIP à réaliser

- **Les deux clients SIP :** PC sur lesquels est installé le softphone X-Lite.
- **Poste attaquant :** PC sur lequel on réalise l'attaque.
- **Machine serveur :** PC sur lequel est installé le serveur de VoIP, Asterisk.

III.6 Installation d'Asterisk

Avant d'installer Asterisk, il faut préparer le système sous lequel on installera notre serveur. Pour cela, il faut installer tout d'abord les pré-requis nécessaires.

III.6.1 Détermination des pré-requis

Les pré-requis nécessaires pour que l'installation du serveur Asterisk s'accomplit avec succès, sont classés dans un tableau ci-dessous :

Nom du packetage	Commande D'installation	Note
GCC 3.x	yum install -y gcc	Nécessaire pour compiler zaptel, libpri et Asterisk
Ncurses-devel	Yum install -y ncurses-devel	Nécessaire pour menuselect
libtermcap-devel	yum install -y libtermcap-devel	Nécessaire pour asterisk
Kernel evelopment Headers	yum install -y kernel-devel	Nécessaire pour compiler zaptel
Kernel development Headers (SMP)	yum install -y kernel-smp-devel	Nécessaire pour compiler zaptel
GCC C++ 3.x	yum install -y gcc-c++	Nécessaire pour asterisk

OpenSSL (optionnel)	yum install -y openssl-devel	Dépendance de OSP, IAX2 encryption, res_crypt (RSA key support) Nécessaire pour asterisk
zlib-devel (optionnel)	yum install -y zlib-devel	Dépendance de DUNDi Nécessaire pour asterisk
unixODBC; unixODBC-devel (optionnel)	yum install –y unixODBC-devel	Dépendance de func_odbc, cdr_odbc res_config_odbc, res_odbc, ODBC_STORAGE
Libtool(optionnel; recommandé)	yum install -y libtool	Dependence de ODBC-related modules
GNU make (version 3.80ou plus)	yum install -y make	Nécessaire pour compiler zaptel et asterisk

Tableau I.1 : Liste de paquetages nécessaires pour compiler Asterisk,Llibpri et Zaptel

Le meilleur chemin pour obtenir le code source d'Asterisk et ces paquetages est de les télécharger à partir du site web **www.asterisk.org**

On peut aussi les télécharger directement du serveur de Digium [13].

III.6.2 Téléchargement des codes sources

Voilà les lignes de commandes nécessaires pour le téléchargement d'Asterisk, libpri et zaptel On identifie l'url. Après on télécharge via la commande wget

```
# cd /usr/src/
# wget http://downloads.digium.com/pub/asterisk/asterisk-1.8-current.tar.gz
# wget http://downloads.digium.com/pub/libpri/libpri-1.4-current.tar.gz
# wget http://downloads.digium.com/pub/zaptel/zaptel-1.4-current.tar.gz
```

III.6.3 Extraction des paquetages

Les paquetages téléchargés sont des archives compressés qui contiennent le code source, on aura besoin de les extraire, en utilisant la commande tar, avant de les compiler

```
# cd /usr/src/
# tar zxvf zaptel-1.4-current.tar.gz
# tar zxvf libpri-1.4-current.tar.gz
# tar zxvf asterisk-1.8-current.tar.gz
```

III.6.4 Compilation et installation:

Le Zaptel est un noyau chargeable qui présente une couche d'abstraction entre le matériel et les pilotes de Zapata dans le module Asterisk.

```
# cd /usr/src/zaptel-1.4.2          =accès au dossier de Zaptel
# make clean                        =supprime les fichiers inutiles après installation.
# ./configure                       =construction d'un nouveau fichier makefile.
# make menuselect                   =exécution de la partie menuselect dans le fichier make
file
# make                              =compilation du code source
# make install                      =exécution de la partie install dans makefile.
```

Makefile est un fichier qui contient les instructions à exécuter à partir des commandes, ./configure, make, make install, make config, etc. chacune de ces commandes exécute le code approprié à elle dans ce fichier.

Libpri est utilisé par les décideurs du multiplexage temporel (TDM) des appareils VoIP, mais même s'il n'y a pas le matériel installé, il est conseillé de compiler et installer cette bibliothèque. Elle doit être compilé et installé avant Asterisk, car elle sera détecté et utilisé lorsqu'Asterisk est compilé [13].

```
# cd /usr/src/libpri-1.4
# make clean
# make
# make install
```

Nous allons maintenant compiler et installer Asterisk.

```
# cd /usr/src/asterisk-1.8.3
# make clean
#. /configure
# make menuselect
# make install
# make samples
```

Dans le cas où on voudrait bien lancer zaptel et le serveur asterisk au démarrage du système, il faut exécuter après la compilation et l'installation des paquetages la commande suivante :

```
# make config          =cette commande charge le serveur Asterisk au démarrage du système
```

Ainsi Asterisk est installé il suffit maintenant de lancer le serveur et de se connecter à la console CLI (Command Line Interface) via la commande :

```
# asterisk –r
```

III.7 Configuration d'Asterisk

III.7.1 Identification des fichiers de configuration

Une fois l'installation d'Asterisk est effectuée, plusieurs fichiers sont créés :

- /usr/sbin/ : Contient le fichier binaire d'Asterisk (programme principal).

- /usr/lib/asterisk/ : Contient les fichiers binaires qu'Asterisk utilise pour fonctionner.

- /usr/lib/asterisk/modules/ : Contient les modules pour les applications, les codecs, et les drivers.

- /var/lib/asterisk/sounds/ : Contient les fichiers audio utilisés par Asterisk, par exemple pour les invites de la boite vocale.

- /var/run/asterisk.pid : Fichier contenant le numéro du processus Asterisk en cours.

- /var/spool/asterisk/outgoing/: Continent les appels sortants d'Asterisk.

- /etc/asterisk/ : Contient tous les fichiers de configuration.

Le dernier dossier nous intéresse vu qu'il contient les fichiers de configuration du serveur Asterisk, parmi ces fichiers on trouve :

- agents.conf: Contient la configuration de l'utilisation des agents, comme dans le cas d'un centre d'appel. Ceci nous permet de définir les agents et de leurs assigner des ID et des mots de passe.
- asterisk.conf: Définit certaines variables pour l'utilisation d'Asterisk. Il sert essentiellement à indiquer à Asterisk où chercher certains fichiers et certains programmes exécutables.
- extensions.conf: Configure le comportement d'Asterisk. C'est le fichier qui nous intéresse le plus dans ce travail.
- iax.conf: Configure les conversations VoIP en utilisant le protocole Inter-Asterisk Exchange (IAX).

- rtp.conf: Ce fichier de configuration définit les ports à utiliser pour le protocole RTP (Real-Time Protocol). Il faut noter que les numéros listés sont des ports UDP.
- sip.conf: Définit les utilisateurs du protocole SIP et leurs options. On peut aussi définir d'autres options globales pour SIP telles que, quels ports utiliser et les timeout qu'on va imposer. Nous focalisons sur ce fichier puisque notre solution est basée sur le protocole SIP.
- zapata.conf: Configure les paramètres de l'interface téléphonique Zapata [13].

III.7.2 Configuration des comptes utilisateurs (users)

Les deux fichiers à configurer sont sip.conf et extensions.conf. Dans le fichier sip.conf, on créera des utilisateurs utilisant le protocole sip pour l'établissement de la connexion, voilà les deux clients que nous avons crée au niveau du fichier :

```
[100]
type=friend                    ; spécifie le type d'utilisateur
secret=100                     ; mot de passe
host=dynamic                   ; spécifie une adresse IP par laquelle
l'utilisateur peut accéder à son compte
defaultip=192.168.0.2          ; adresse IP du client
dtmfmode=rfc2833               ; mode du dtmf
context=sip                    ; spécifie le type de routage à utiliser
callerid= "100"<0550505050>    ; identifiant d'utilisateur
[200]
type=friend
secret=200
host=dynamic
defaultip=192.168.0.3
dtmfmode=rfc2833
```

```
context=sip
callerid="200"<0660606060>
```

Passant maintenant à la configuration du fichier extensions.conf

III.7.3 Configuration des extensions

```
[sip]                ;il faut saisir le nom du context entre crochet
exten=>0550505050,1,Dial(SIP/100,20,tr)      ;20 est la durée en seconde de l'attente avant le décrochage si pas de réponse
exten=>0660606060,1,Dial(SIP/200,20,tr)
```

Si l'appelant compose le numéro 0550505050, il est mit en relation avec le poste dont le numéro est 0550505050 qui utilise le protocole SIP.

Il existe d'autres options qu'on peut ajouter dans le fichier extensions.conf, telles que la boîte vocale et le renvoi d'appel. La syntaxe du fichier est sous le format suivant :

Exten= extension, priorité, commande (paramètre)

- Extension : C'est généralement le numéro de téléphone ou le nom du client.
- Priorité : C'est un numéro qui indique la priorité de la commande, le serveur prend en considération la priorité de la commande en utilisant le numéro inscrit dans la syntaxe.
- Commande : C'est la commande qui peut exister, comme la commande dial (appel), voicemail (boîte vocale), etc.

On peut utiliser plusieurs options pour un seul numéro d'appel, on peut mettre par exemple un transfert d'appel vers un autre numéro ou vers la boite vocale selon des priorités [13].

```
exten => 123,1,Answer
exten => 123,2,Playback  (répondeur)
exten => 123,3,Voicemail(9) (9 est le numéro de la boîte vocale)
exten => 123,4,Hangup
```

Dans chaque ajout ou modification d'un client, il faut mettre à jour le serveur Asterisk en utilisant les commandes suivantes :

```
Localhost*CLI> sip reload
Localhost*CLI> dialplan reload
Localhost*CLI> reload
```

Nous pouvons voir les deux utilisateurs avec la commande suivante :

```
Localhost*CLI> sip reload
```

III.8 Le logiciel X-Lite

III.8.1 Installation

X-Lite est un softphone freeware, son utilisation est simple, il est disponible pour les systèmes d'exploitation Windows et Mac sur le site de l'éditeur CounterPath. Voici le lien du téléchargement du logiciel :

http://www.counterpath.com/index.php?menu=download

L'installation sur windows 7 se fera d'une manière classique.

III.8.2 Configuration de X-Lite

Pour configurer le client X-Lite nous devons procéder comme suit :

Lancer X-Lite, puis cliquer sur « Softphone » puis sur « Account Settings » [01].

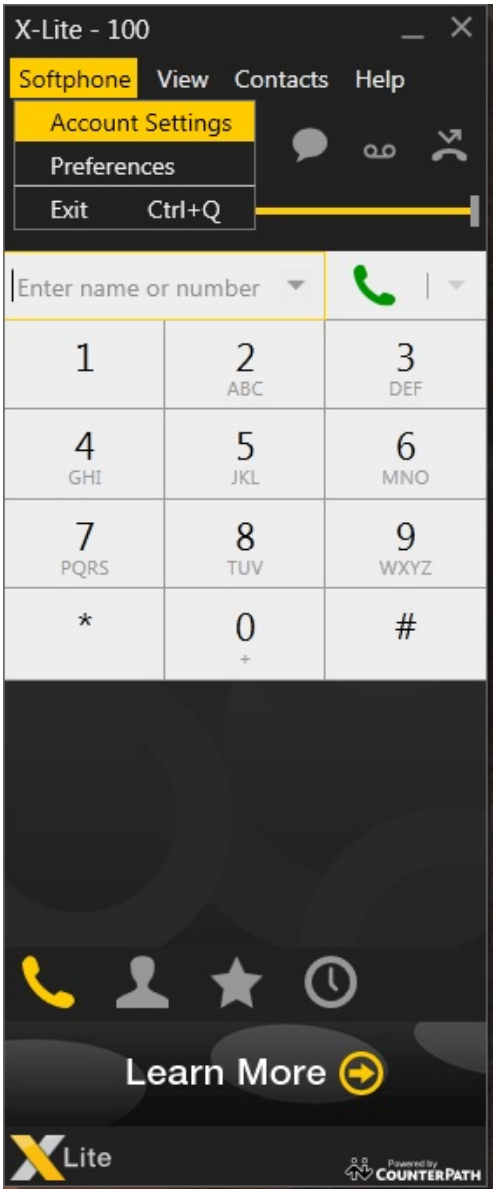


Figure III.3 : logiciel X-lite

Dans la fenêtre qui s'ouvre, il suffit de remplir les champs illustré suivant des deux utilisateurs :

L'utilisateur 100 :

- Identifient servant a loguer l'utilisateur (User ID) : 100
- Mot de passe associé (Password) : 100
- Identifiant affiché pour l'utilisateur (Display Name) : 100
- Nom de domaine (Domain) : 192.168.0.1
- Nom sous lequel l'autorisation d'accès est possible (Authorization name) : 100

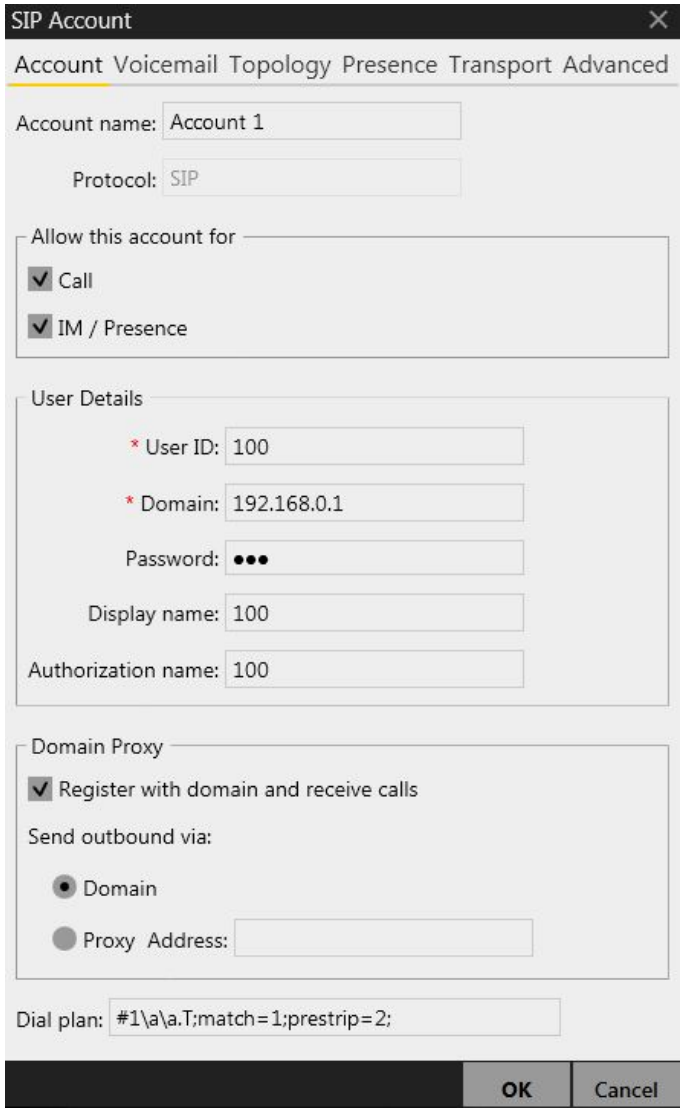


Figure III.4: Configuration de compte du client « 100 »

Et la même chose pour l'utilisateur « 200 ».

Il est à noter qu'afin que l'authentification soit possible, ces valeurs doivent être conformes à celles saisies dans le fichier sip.conf du serveur Asterisk.

Une fois la configuration est achevée, le softphone se connectera automatiquement au serveur et s'enregistrera communications sont désormais possibles. Sinon, un message d'erreur explique le motif qui a fait échouer le processus [13].

Nous pouvons maintenant faire un appel test de l'utilisateur « 100 » vers l'utilisateur « 200 » comme ceci :

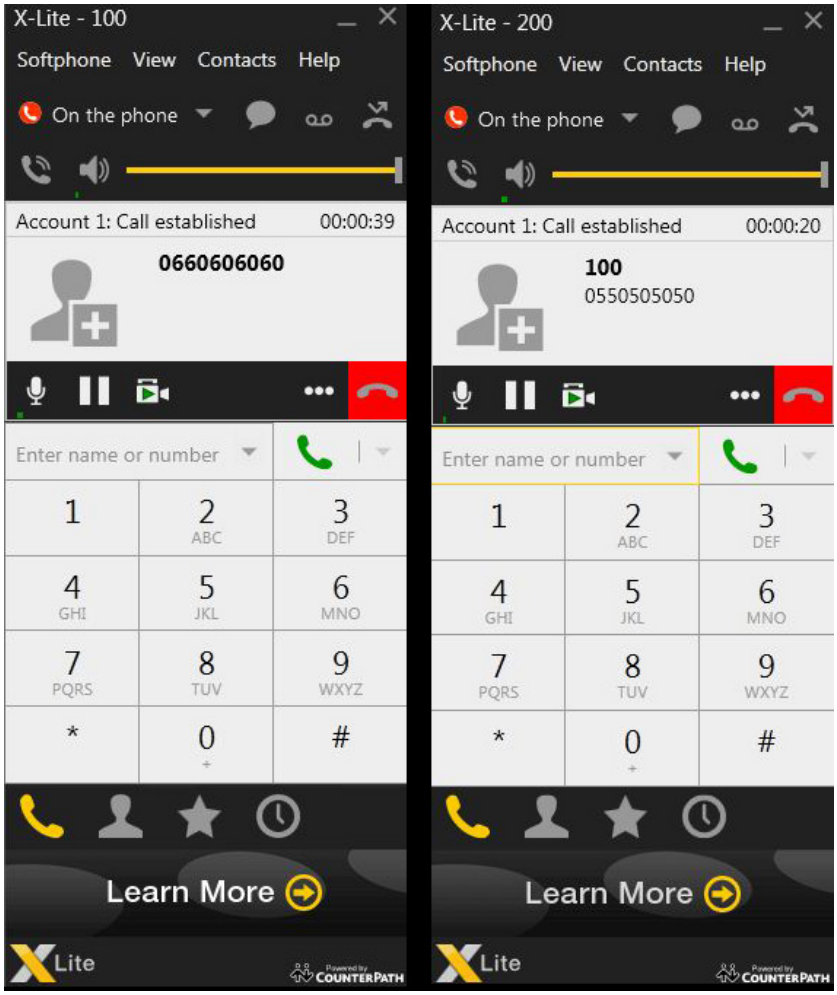


Figure III.5 : Appel test entre l'utilisateur « 100 » et « 200 »

III.9 Discussion

On peut dire qu'Asterisk est un outil ouvert à tous, gratuit et simple d'utilisation. On a pu procéder à son installation et sa configuration sans trop de difficulté.

On a pu faire des tests d'appels entre deux clients X-Lite et ce avec une simplicité d'utilisation.

Chapitre IV

Sécurisation de la solution mise en place

IV.1 Préambule

Après avoir étudié les protocoles de la VoIP et identifié les vulnérabilités qui menacent ces systèmes. Dans ce chapitre, nous présentons quelques techniques suivies par l'attaquant. Nous réalisons un exemple d'attaque sur le réseau VoIP, ensuite nous nous intéressons aux techniques, mécanismes et configurations à mettre en place dans le but de sécuriser la solution VoIP basée sur le serveur Asterisk.

IV.2 Localisation des serveurs VoIP

Toute bonne attaque VoIP commence par une étape qui établit le profil de la cible connu sous le nom profiling ou encore foot printing. Une empreinte englobe les informations sur la cible qui déploie le serveur VoIP et ces paramètres de sécurité.
Il existe plusieurs méthodes pour la collecte des informations en voici quelques-unes des plus utilisées :

IV.2.1 Utilisation des serveurs Whois

Les whois sont des services proposés gratuitement en ligne permettant d'obtenir des informations sur un domaine particulier, sur une adresse de messagerie. Grâce à ses bases de données comme :

Whois.ripe.net : s'occupe d'attribuer des adresses IP pour l'Europe.

Whois.apnic.net : attribue les adresses IP pour l'Asie.

Whois.nic.mil : attribue les adresses IP des systèmes militaires américains.

IV.2.2 Utilisation des aspirateurs de sites

Si la cible a un site, le pirate doit le parcourir à la recherche d'adresses emails, de compte et mots de passes ou d'autres informations précises. Parcourir le code source peut aussi recenser des informations qui pourraient permettre de remonter aux sources. Les aspirateurs de sites permettent d'automatiser ces recherches

IV.2.3 Utilisation des moteurs de recherches et des agents intelligents

Un des grands avantages des moteurs de recherches Internet est leurs énormes potentiels pour découvrir les plus obscurs des détails sur l'Internet. L'un des plus grands risques pour la sécurité est aujourd'hui l'énorme potentiel des moteurs de recherche pour découvrir les détails sur l'Internet. Il existe une variété de façons qu'un hacker peut exploiter en utilisant simplement les fonctionnalités avancées d'un service tel que Google. Le ciblage des catégories suivantes des résultats de recherche peuvent souvent fournir de riches détails sur la solution VoIP déployée par un organisme:

- Vendeur de produit VoIP, les communiqués de presse et des études de cas
- CV de l'administrateur ou liste de références des vendeurs
- Les forums

IV.2.4 Balayage (Scan) des réseaux VoIP

Pour pouvoir identifier chaque composante du réseau, il faut déchiffrer et comprendre un bon nombre de paquets afin de reconnaitre par exemple leur adresse IP et son ID. D'autant plus qu'un réseau VoIP ne se limite pas à quelques clients et un serveur Asterisk. Les serveurs TFTP par exemple sont d'une nécessité pour un attaquant afin de retrouver les fichiers de configurations des téléphones IP pour leur usurper leurs identités par exemple.

Afin de scanner un réseau, l'outil nécessaire pour cela est un scanner de réseau (sniffer en anglais). C'est un logiciel permettant de découvrir les équipements présents sur un réseau et les services qu'il offre. Le scanner est souvent utilisé par les administrateurs réseau au cours de test de sécurité. Son principe de fonctionnement est de tester chaque adresse IP et chaque port TCP ou UDP afin de vérifier la présence d'un serveur ou d'un quelconque équipement fonctionnant en TCP/IP [17].

IV.3 Le logiciel d'attaque (Wireshark)

IV.3.1 Présentation du logiciel

Wireshark est un logiciel libre d'analyse de protocole, utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro ingénierie, mais aussi le piratage. C'est l'analyseur réseau le plus populaire du monde. Cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sur un réseau.

L'utilisation de Wireshark dans notre projet est pour la détection des vulnérabilités dans le réseau VoIP. Nous essayerons de capturer les paquets qui circulent pour déterminer quelques informations telles que les adresses IP, les numéros de ports, et d'autres informations qui servent au piratage (vol d'identité, dénie de service, etc.). Ainsi que nous pouvons écouter une communication entre deux clients en décodant les paquets RTP (écoute clandestine) [11].

IV.3.2 Captures de trames

Nous avons placé Wireshark dans une 3éme machine qui va jouer le rôle de l'attaquant. Elle va sniffer tous le trafic circulant dans notre réseau local. Nous avons lancé au début la capture des trames ensuite on a initialisé une connexion entre deux clients, « 200 » et « 100 ».On obtient ce résultat :

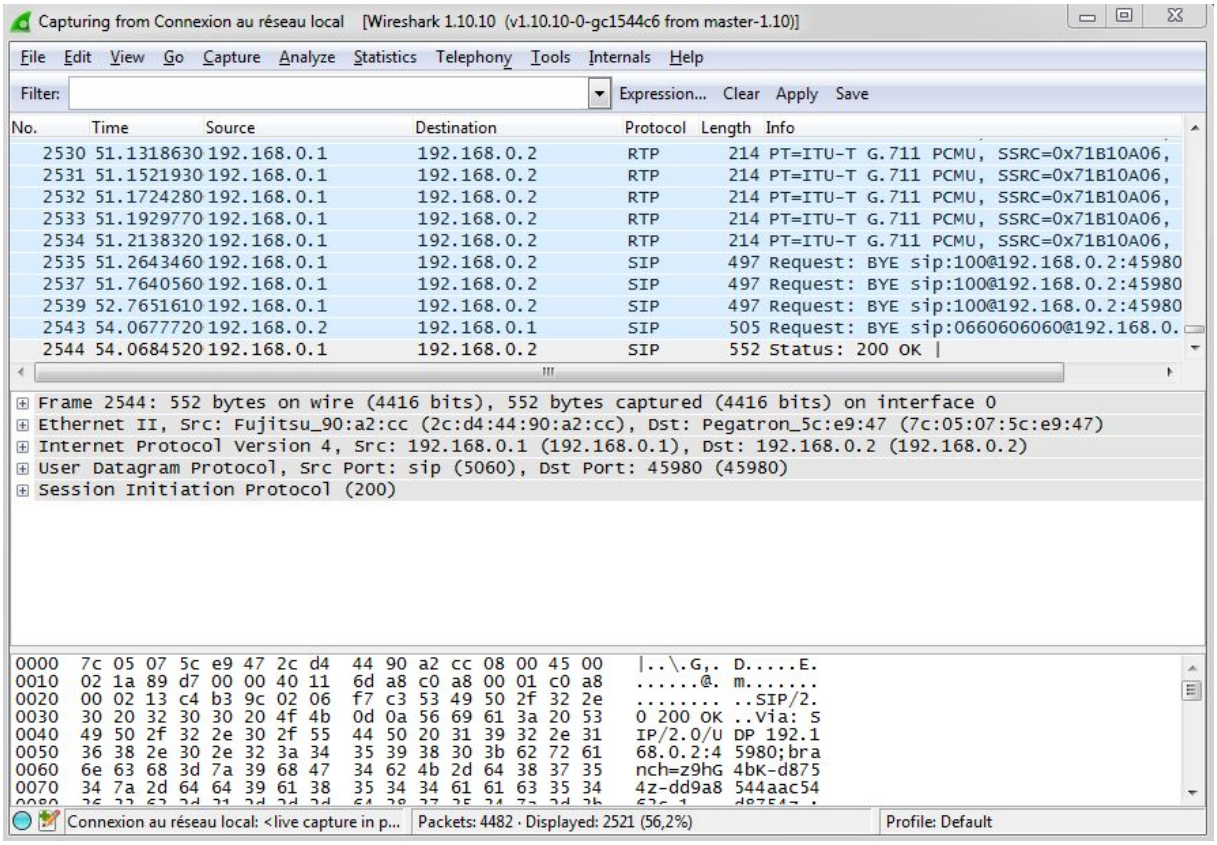


Figure IV.1 : Ecran de Wireshark

Comme nous pouvons le voir dans la figure IV.1, la conversation entre ces deux hôtes a été capturée. La fenêtre principale de Wireshark comprend deux grandes parties. Dans la première partie, nous voyons les différentes étapes de connexion entre les deux clients. Dans la deuxième partie, celle la plus intéressante, nous pouvons lire le contenue des paquets et donc collecter des informations très indispensables pour effectuer une bonne attaque.

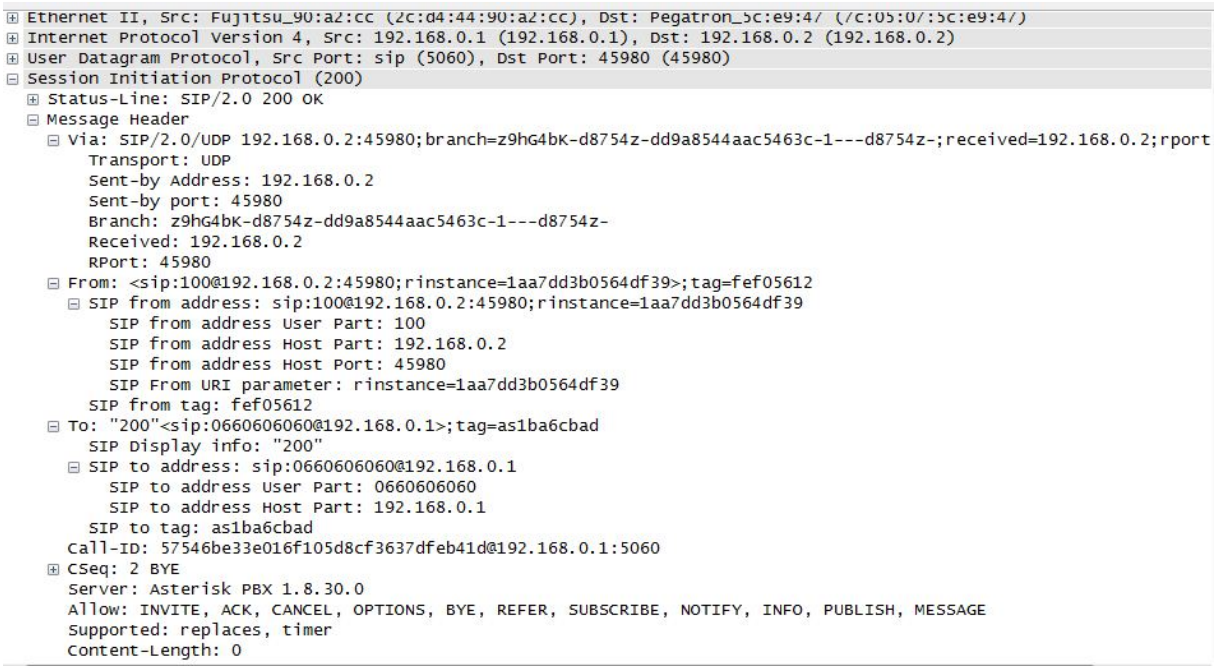


Figure IV.2: Exemple de paquet qui contient une requête INVITE

Dans la figure IV.2, le paquet que nous avons choisi pour examiner. Celui-ci est un paquet utilisant le protocole SIP contenant une requête INVITE. Cette requête contient des informations indispensables dans le cas où nous voulons effectuer une attaque basée sur le protocole SIP. Par exemple dans le cas où nous voulons exécuter une attaque de type DoS en utilisant le protocole SIP, nous aurions besoin de connaitre le user agent. Dans cet exemple il n'est autre que le serveur Asterisk, l'adresse SIP de notre victime, son identité et d'autres paramètres.

IV.3.3 Démonstration de l'attaque clandestine avec Wireshark

Nous utilisons Wireshark dans cette sous-section pour conduire l'attaque d'écoute clandestine. Cette attaque consiste à capturer les trames circulant entre deux machines effectuant une conversation VoIP, et décoder par la suite les paquets afin d'écouter la conversation effectuée.

Nous allons maintenant procéder au décodage de l'appel. Dans le menu de Wireshark, nous cliquons sur le bouton « Telephony », puis ensuite le bouton « VoIP Calls »

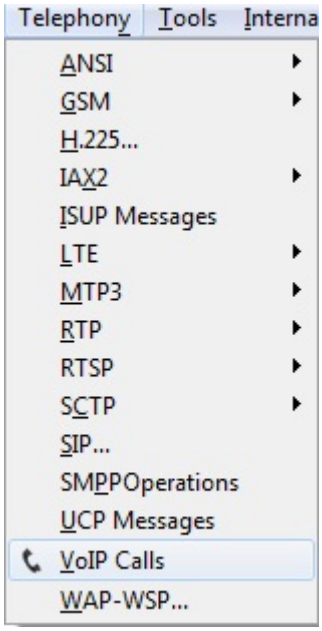


Figure IV.3 : accéder au décodage d'appel

Une deuxième fenêtre s'ouvre contenant les communications :

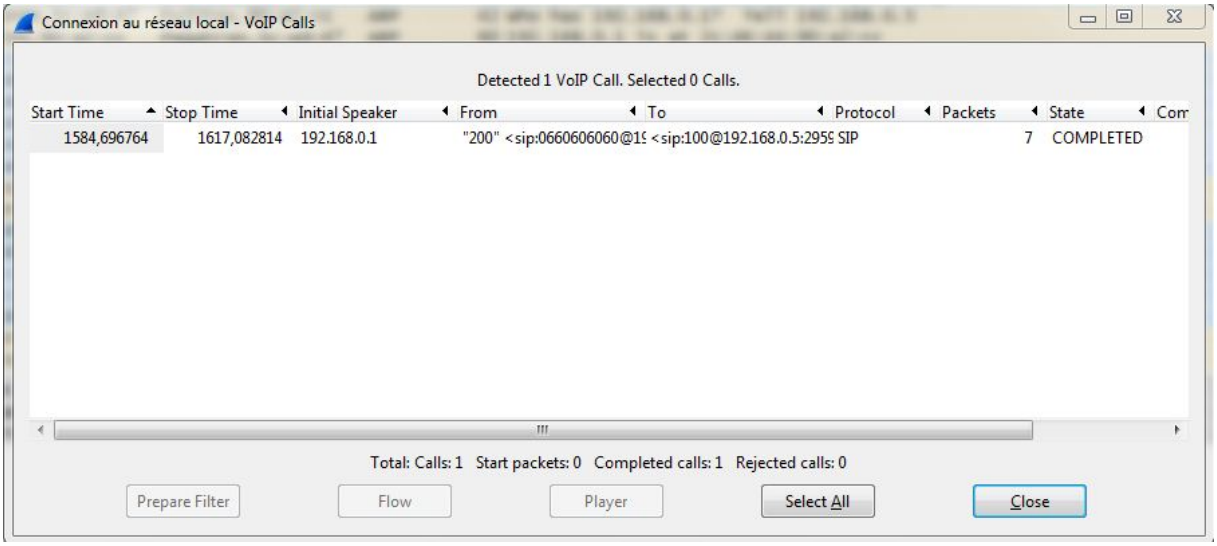


Figure IV.4 Communication téléphonique détectés

Nous cliquons sur le bouton « Player », une fenêtre « RTP Player » s'ouvre pour le décodage nous cliquons sur « Decode » et nous obtenons ceci :

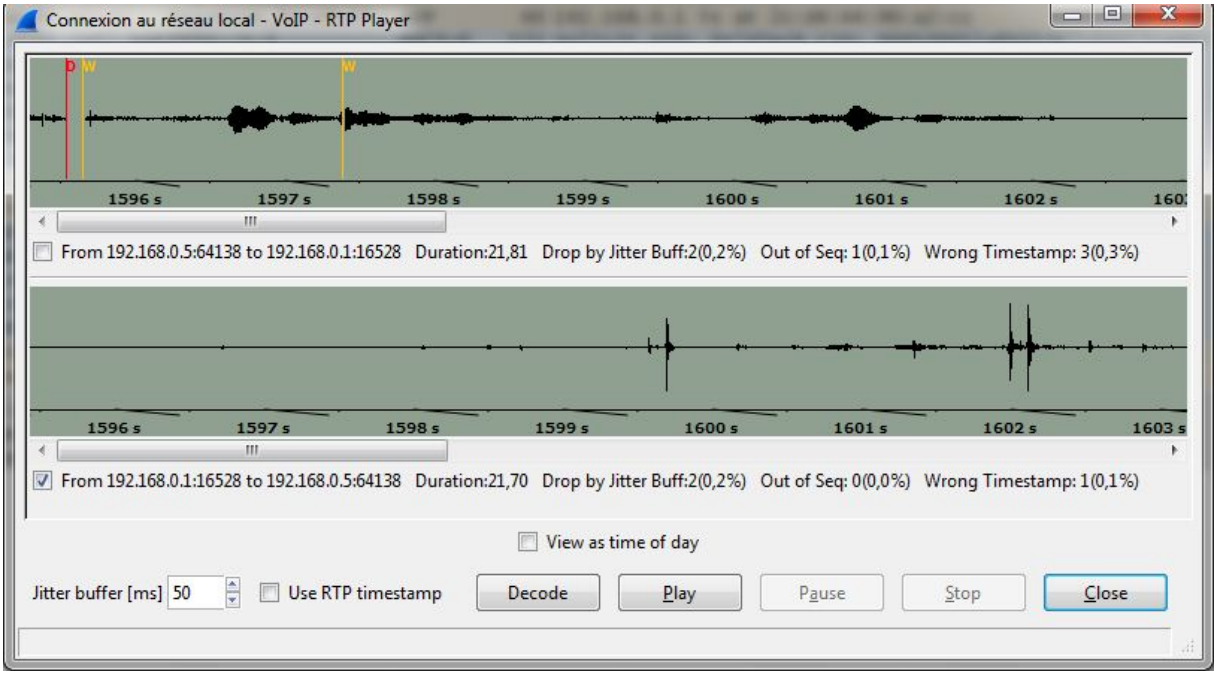


Figure IV.5 Communication décodé (RTP Player)

Maintenant que le décodage a abouti nous pouvons aussi voir sur la figure IV.5 que le son est décodé et qu'il est prêt à être écouté en appuyant sur le bouton « Play » [11].

IV.4 Choix et implémentation des bonnes pratiques

Pour se protéger contre des attaques, nous avons choisi un ensemble de solutions qui peuvent aider à minimiser les menaces.

IV.4.1 Bonne pratique contre l'écoute clandestine

IV.4.1.1 Implémentation du protocole SRTP

Parmi les solutions les plus performantes et les plus faciles à mettre en œuvre, pour contourner l'attaque de l'Eavesdropping ou l'écoute clandestine, est l'implémentation du protocole SRTP sur le serveur Asterisk. En effet, ce protocole permet de chiffrer les données et de les injecter dans le trafic. De cette façon une personne malveillante essayant de décoder les paquets, ne pourra plus user de cette attaque. Il faut savoir que SRTP est une branche d'Asterisk et donc on aura besoin de le récupérer depuis le serveur SVN (subversion). Subversion est un système de gestion de version, c'est-à-dire qu'il permet de gérer la version d'un fichier source ou de garder un historique de

toutes ces versions. Voici les étapes à suivre pour la configuration de SRTP sur Asterisk :

Avant de commencer la configuration, il faut compiler et installer la librairie de SRTP

LIBSRTP :

```
# tar -xzf srtp-1.4.2.tgz                    =décompression des paquetages
 # ./configure --prefix=/usr make      =installation des composants binaires de la librairie dans  le répertoire /usr
# make runtest
# make install
```

Ensuite il faut installer la librairie **MINISIP libraries :**

```
# svn co -r3250 svn://svn.minisip.org/minisip/trunk minisip-trunk      =commande permettant de récupérer une révision ainsi que ses métadonnées depuis le dépôt
# cd minisip-trunk
```

Une révision est une instance d'un fichier à un moment donné. Une métadonnée est une donnée servant à définir ou décrire une autre donnée .

Ensuite il faut installer et compiler **libmutil** :

Mais d'abord il faut lancer le script de démarrage pour générer le script de configuration.

```
# cd libmutil
# libmutil$ ./bootstrap          =charger la librairie dans le rom
```

Ensuite il faut compiler le code source de **libmutil** et l'installer:

```
# libmutil$ ./configure --prefix=/usr      =installation des composants binaires de la librairie  dans le répertoire /usr)
# libmutil$ make
```

Aussi il faut compiler et installer les librairies, libmnetutil, libmcrypto, libmikey. La compilation et installation de ces librairies se fait de la même façon que la librairie **libmnetutil:**

```
# cd ../libmnetutil
# libmnetutil$ ./bootstrap            =charger la librairie dans le rom
# libmnetutil$ ./configure --prefix=/usr (installation des composants binaires de la librairie dans le répertoire /usr)
# libmnetutil$ make
# libmnetutil$ make install
```

Passons maintenant à la configuration d'Asterisk en lui ajoutant les correctifs et les fichiers nécessaires ainsi que l'ajout du module SRTP dans le menu d'Asterisk.

```
# svn checkout -r61760 http://svn.digium.com/svn/asterisk/trunk asterisk-trunk
# cd asterisk-trunk
#wget http://bugs.digium.com/file_download.php?file_id=13837&type=bug
=Télécharger un fichier depuis cette url
# patch -p1 < ast_srtp_r61760_mikey_r3250.patch            =l'application d'un patch sur le serveur Asterisk
# ./bootstrap.sh          =compilateur permettant de lancer le compilateur de configuration du menu d'Asterisk
# ./configure
# make menuselect                =vérifier res_srtp dans "resource modules"
# make
# make install
```

Ensuite il faut configurer les fichiers **sip.conf** et **extensions.conf**:

- **extensions.conf**

[main]

Le fichier permettant le routage doit être au courant que nous allons utiliser le protocole SRTP pour cela nous devons rajouter cette option dans le fichier. Il faut aussi créer un test sur le port 7 appelé port écho qui permettra de trouver les causes des problèmes liés a la piles TCP / IP dans le cas où il y'a des problèmes de connexion. Cette configuration s'applique à l'utilisateur ayant pour numéro 0550505050 (utilisateur « 100 »). Dans cet exemple SRTP est utilisé optionnellement :

```
exten =>0550505050,1,Set(_SIPSRTP=optional)                    ; l'utilisation de SRTP est optionnel
exten =>0550505050,2,Set(_SIPSRTP_CRYPTO=enable)               ; activer le cryptage
exten =>0550505050,3,Playback(demo-echotest)                   ; création d'un test echo permettant de savoir si oui ou non la connexion a eu lieu
exten =>0550505050,4,Echo                                      ; faire le test echo
exten =>0550505050,5,Playback(demo-echodone)                   ; si le test echo a réussi cette option nous permettra d'écouté le son qu'on a créé pour le test
exten =>0550505050,n,hangup
```

Cette configuration s'applique à l'utilisateur ayant pour numéro 0660606060, c'est donc l'utilisateur
« 200 » :

```
exten =>0660606060,1,Set(_SIPSRTP=require)    ; l'utilisation de SRTP est requise
exten =>0660606060,2,Set(_SIPSRTP_MIKEY=enable)
exten =>0660606060,3,Playback(demo-echotest)
exten =>0660606060,4,Echo
exten =>0660606060,5,Playback(demo-echodone)
exten =>0660606060,n,hangup
```

• **sip.conf**

Dans ce fichier l'option à modifier dans les paramètres des clients est la suivante :

```
context=main        ; le main fait référence à la configuration que nous venons de créer
dans le fichier extensions.conf et donc le routage choisi
```

Pour finir voici quelques remarques à prendre en considération dans le cas où nous voulons utiliser SRTP avec le serveur Asterisk :

- MIKEY ne prend pas en charge le cryptage en option.
- L'appelé ne peut pas sélectionner la méthode de cryptage

IV.4.1.2 Mise en place de la solution VPN

Autre solution pour crypter le trafic dans notre réseau, est l'implémentation d'un VPN au sein des machines utilisées pour la VoIP.

Ce dernier qui permet de véhiculer du trafic crypté grâce à des clés de cryptage ce qui rend leur déchiffrage presque impossible par une tierce partie. Un VPN permettra donc de contourner les attaques d'écoute clandestine.

OpenVPN est un logiciel « open source » permettant de créer un réseau virtuel basé sur SSL. Il peut être utilisé afin de relier deux réseaux ou plus via un tunnel chiffré à travers l'Internet. Par ailleurs, OpenVPN n'utilise pas de protocole de communication standard. Il faut donc utiliser un client OpenVPN pour se connecter à un serveur OpenVPN.

• **Installation d'OpenVPN**

L'installation d'OpenVPN se fait grâce à la commande suivante :

```
# yum install –y openvpn        =l'option –y permet d'accepter l'installation directement
```

- **Générations des certificats**

Maintenant et après l'installation, il faut créer les certificats et les clés qui vont permettre aux clients et au serveur de s'authentifier mutuellement de telle sorte que personne d'autres ne puisse se connecter au VPN.

```
# cd /usr/share/openvpn/easy-rsa/
```

En suite il faut nettoyer le répertoire /keys avant la génération des nouveaux certificats et relancer la prise en charge des nouvelles variables grâce à la commande suivantes :

```
# .. /vars
#./clean-all
```

Création des certificats

D'abord il faut commencer à créer l'autorité de certification en tapant la commande suivante :

```
# . /build-ca
```

Maintenant nous allons créer le certificat pour le serveur avec la commande suivante :

```
# ./build-key-server server
```

Création de certificat pour le client avec la commande suivante :

```
# ./build-key client
```

Maintenant au tour de la génération de clés secrètes à travers des canaux non sécurisés avec la création des paramètres Diffie-helmann qui se fait comme suit :

```
# ./build-dh
```

En suite copiant l'ensemble des informations cryptographiques, que nous venons de générer dans le répertoire keys avec la commande suivante :

```
# cp Keys/* /etc/openvpn
```

- **Création d'un utilisateur OpenVPN**

L'utilisateur **OpenVPN** sera chargé de lancer le service de telle sorte que même si nous nous font pirater la machine, l'attaquant n'aura que les droits de cet utilisateur et pas avec les droits root.
Il faut créer un groupe d'utilisateur dans lequel nous allons affecter l'utilisateur grâce à la commande suivante :

```
# groupeadd openvpn          =le groupe qu'on vient de créer se nomme openvpn
Ensuite créer l'utilisateur
# useradd –d /dev/null –s /bin/false –g openvpn
```

- **Configuration et lancement du serveur**

Il faut tout d'abord copier le fichier server.conf se trouvant dans le répertoire /usr/share/doc/openvpn-2.1/sample-config-files et le placer dans le répertoire suivant /etc/openvpn :

```
# cp server.conf /etc/openvpn
```

Éditer ce fichier pour y positionner les variables pour la mise en place du VPN.

```
# Vi server.conf (éditer les paramètres du fichier)
```

Les paramètres à modifier :

- **Dev tun**

  Pour pouvoir utiliser OpenVPN en mode tunnel

Server 10.8.0.0 255.255.255.0

A chaque fois qu'un client se connectera au vpn, le serveur lui attribuera une adresse IP contenue dans cette plage.

- **Comp-lzo** compression des données.
- **User openvpn / group openvpn** lancer le serveur.

Une fois sauvegarder et lancer le service on passe à la configuration du côté du client [17].

Configuration du client

La configuration se fait comme suit :
Installer le client OpenVPN sur la machine. Ensuite copier les fichiers suivant (Ca.crt, Client.crt, Client.csr et Client.key) qui se trouvent sous le répertoire /etc/openvpn du côté serveur.
En suite configurer le fichier **client.conf** pour la reconnaissance du serveur avec l'ajout dans le fichier de :

```
Remote 172.16.64.26 1194
```

C'est l'adresse du serveur et le port sur lequel va s'effectuer la connexion VPN.

Alors qu'avec cette dernière le réseau VPN est prêt à être utiliser entre le serveur Asterisk et ces clients.

IV.4.2 Bonne pratique contre le DOS – BYE

La bonne pratique contre les attaques DOS permet de limité ces attaques et minimisé la vulnérabilité du réseau et non la sécurité totale de ce dernier.

Pour cela notre choix est fait sur un **pare-feu Netfilter**

IV4.2.1 Implémentation d'un firewall Netfilter

Un firewall efficace doit posséder plusieurs interfaces réseaux pour pouvoir faire un filtrage entre plusieurs zones.
Le firewall va nous permettre de minimiser le trafic entrant au serveur Asterisk et cela pour limiter les attaques de types DoS. Qui est notre objectif de ne laisser passer que le trafic VoIP et plus exactement les paquets basés sur le protocole SIP et le protocole RTP.
Et comme on a un firewall au niveau du serveur, alors que toutes les requêtes en direction du serveur Asterisk passeront automatiquement par ce firewall.
IPtable est la commande permettant de paramétrer le filtre Netfilter du noyau Linux et donc de configurer le Firewall.

La commande suivante permet de programmé notre firewall pour qu'il puisse laisser passer seulement le trafic VoIP au niveau du serveur Asterisk et de bloquer tous le trafic restant.

```
# iptables -A INPUT -p udp -m udp --dport 5060 -j ACCEPT
```

Cette commande va permettre d'accepter le trafic UDP entrant du port 5060.(port du protocole 20000 -j ACCEPT sip)

```
# iptables -A INPUT -p udp -m udp --dport 10000:
```

Cette commande permet d'accepter le trafic UDP entrant du protocole RTP.

Attribuer une règle par défaut pour bloquer tous le trafic restant et qui passe par UDP avec :

```
# iptables -A INPUT -p UDP -j DROP
```

IV.4.2.2 Exécuter Asterisk sous un utilisateur non privilégié :

Changer l'utilisateur sur lequel Asterisk tourne est l'une des bonnes pratiques pour sécuriser notre serveur Asterisk.

Objectif :

Si le serveur Asterisk est compromis au niveau de sa sécurité ceci ne doit en aucun cas affecter toute la machine sur laquelle tourne le serveur.

Les étapes à suivre :

Première étape est d'arrêter Asterisk avec :

```
# /etc/init.d/asterisk stop #> Shutting down asterisk: OK
```

Ensuite, créer un utilisateur depuis lequel Asterisk va démarrer (Nous avons choisie groupe Asterisk et comme nom d'utilisateur Asterisk)

```
# /usr/sbin/groupadd asterisk
#/usr/sbin/useradd -d /var/lib/asterisk -g asterisk asterisk
```

Ensuite, attribuer les droits d'accès pour Asterisk, Les fichiers se trouvant dans le répertoire **/var/spool/asterisk** doivent être la propriété de l'utilisateur Asterisk et accessibles en écriture.

Accession des répertoires : /var/lib/asterisk , /var/log/asterisk, /var/run/asterisk, /var/spool/asterisk, /usr/lib/asterisk et le dossier /dev/zap se fait comme suit :

```
# chown --recursive asterisk:asterisk /var/lib/asterisk
# chmod --recursive u=rwX,g=rX, /var/lib/asterisk
```

La commande **--recursive** permet de modifier les permissions d'un répertoire et de ses sous-répertoires. Ainsi grâce à la commande **chown** le propriétaire du répertoire /var/lib/asterisk et ses sous-répertoires est devenue asterisk.

Lecture du répertoire /etc/asterisk et son contenu afin de modifier avec :

```
# chown --recursive root:asterisk /etc/asterisk
# chmod --recursive u=rwX,g=rX, /etc/asterisk
```

Ensuite, changer le répertoire d'Asterisk afin qu'il puisse démarrer du nouveau chemin crée:

```
# cp /etc/asterisk/asterisk.conf /etc/asterisk/asterisk.conf.org
# vi /etc/asterisk/asterisk.conf
```

Modifiant Le chemin en changeant la ligne:

```
astrundir => /var/run à astrundir => /var/run/asterisk
```

En suite activant le nouveau groupe et l'utilisateur que nous avons crées

```
# cp /etc/init.d/asterisk /etc/init.d/asterisk.org
# vi /etc/init.d/asterisk
```

Changeant la ligne suivante afin d'informer Asterisk de son nouveau utilisateur:

```
#AST_USER="asterisk"
#AST_GROUP="asterisk"
à
AST_USER="asterisk"
AST_GROUP="asterisk"
```

Maintenant redémarrant Asterisk avec les nouveaux paramètres :

```
/etc/init.d/asterisk restart
asterisk -U asterisk -G asterisk
```

IV.4.2.3 Configuration des fichiers sip.conf et extensions.conf

Le cryptage de mot de passe de l'utilisateur ou client est autre bonne pratique pour mieux assurer la sécurité du serveur Asterisk.

Grâce au cryptage le mot de passe du client devient illisible dans le cas où une personne malveillante accède au fichier **sip.conf.**

Le cryptage se fait avec la commande suivante :

```
echo - n "<user>:<realm>:<secret>" | md5sum
```

Nous pouvons aussi assurer la sécurité du serveur en attribuent des privilèges et des limites d'accès au utilisateur et cela s'effectue au niveau du fichier **sip.conf**. Cela nous permet de limiter les attaques de types DoS en limitant les requêtes d'invitation vers le serveur avec la configuration d'un utilisateur comme suit :

```
[general]
allowguest=no
```

allowguest=no interdiction de l'accès à toutes personnes non authentifié.

On peut aussi contrôler les appels au niveau des comptes des utilisateurs.

Example :

Utilisateur nommé « 100 »

```
[100]
type=friend
md5secret=bed1e076ced1aadeba7e151240c7a955
host=dynamic
defaultip=192.168.0.1
canreinvite=no
```

Avec ces instructions, un utilisateur ne peut effectuer qu'une seule invitation durant un appel

Une autre possibilité en contrôlant l'authentification :

```
insecure=no
```

Et cela pour avoir un maximum de sécurité, en le mettant en NO, le serveur interrogera toujours pour l'authentification à chaque nouvelle connexion du client vers le serveur.

On peut aussi limiter le nombre d'appels avec :

```
call-limit=1
```

Cette instruction permet de limiter le nombre d'appels sortant ou rentrant a un seul ce qui permet de contourner les attaques de types DoS visant le serveur Asterisk [17].

Discussion :

Tout au long de ce chapitre, nous avons pu tester un exemple d'attaque en sniffant le trafic du réseau et présenté des différentes mesures de sécurisation pour le réseau VoIP contre des plusieurs attaques afin de pouvoir les éviter.

Mais à savoir qu'il est impossible d'en avoir une sécurité maximale au sein du réseau VoIP.

Conclusion générale

Après avoir étudié la voix sur IP et présenté la solution mise en place, l'objectif de ce projet est de sécuriser un réseau VoIP avec cette solution mise en place. L'étude débutée par l'installation et la configuration de la solution, en suite effectuer des attaques sur le réseau VOIP afin de pouvoir le sécurisé.

On a constaté que la sécurisation totale de notre solution est quasi impossible. La sécurité de la Voix sur IP est un sujet critique qui pose des problèmes difficiles à résoudre. Avec l'intégration de la téléphonie dans les systèmes d'information et dans le monde des réseaux IP, la sécurisation de cette application devient particulièrement complexe. Les besoins concernent l'authentification, la confidentialité, l'intégrité, la protection contre l'usurpation d'identité, le respect de la vie privée ou encore la non répudiation.

La question n'est donc pas de savoir si la sécurité est nécessaire, mais comment se mettre en place une solution robuste et interopérable avec les infrastructures existantes. Chaque jour, la cybercriminalité nous rappelle que la sécurité n'est plus une option mais une obligation.

Acronymes

ACE = Access Control Entry

ACL = Access Control List

AH = Authentification Header

ARP = Address Resolution Protocol

CAN = Convertisseur analogique numérique

CLI = Command Line Interface

DDoS = Distributed Denial of Service

DHCP = Dynamic Host Configuration Protocol

DMZ = Démilitarized Zone

DNS = Domain Name System

DoS = Deny of Service

DTMF = Dual-Tone Multi-Frequency

ESP = Encapsulated Security Payload

FTP = File Transfer Protocol

GSM = Global System for Mobile Communications

HTTP = HyperText Transfer Protocol

IAX = Inter-Asterisk Exchange

ICMP = Internet Control Message Protocol

IETF = Internet Engineering Task Force

IGMP = Internet Group Management Protocol

IGRP = Interior Gateway Routing Protocol

IM = Instant Message

IP = Internet Protocol

ISDN = Integrated Service Data Network

ITU = International Telecommunications Union

LAN = Local Area Network

MD5 = Message Digest 5

MIKEY = Multimedia Internet KEYing

NAT = Network Address Translation

PABX = Private Automatic Branch eXchange

PBX = Private Branch eXchange Network

PSTN = Public Switched Telephone

QoS = Quality of Service

RFC = Requests For CommentRNIS = Réseau Numérique à intégration de Service

RTC = Réseau Téléphonique de Commuté

RTCP = Real-time Transport Control Protocol

RTP = Real-Time Transport Protocol

RTSP = Real Time Streaming Protocol

SIP = Session Initiation Protocol

SNMP = Simple Network nagement Protocol SRTP = Secure Real-time Transport Protocol

TCP = Transport Control Protocol

TDM = Time division Multiplexing

TFTP = Trivial File Transfert Protocol

TLS = Transport Layer Security

ToIP = Telephony over Internet Protocol

UAC = User Agent Client

UAS = User Agent Server

UDP = User Datagram Protocol

URL = Uniform Resource Locator

VoIP = Voice over Internet Protocol

VPN = Virtual Private Network

Bibliographie

[01 D. Ourabah, M. guillet, L. Lecouley, V. Batouflet, W. Zivic, « Asterisk ». Rapport de projet, 2006.

[02] A. Hakim, D.Adrien, D. Sidney, « La protection des réseaux contre les attaques DoS ». Mai 2009.

[03] Site web : http://www.frameip.com/voip

[04] Site web : http://doc.ubuntu-fr.org/asterisk

[05] Site web : http://fr.wikipedia.org/wiki/Session_Initiation_Protocol

[06] Site web : http://wiki.wireshark.org/VoIP_calls

[07] S. Ben Ahmed, « Intégration de Radius dans un réseau VoIP avec Asterisk ». Mémoire de fin d'étude, 2008.

[08] Site web : http://ts5ri-voip-pfe.fr.gd/Protocole-H-.-323.htm

[09] Site web : http://ts5ri-voip-pfe.fr.gd/Protocole-SIP.htm

[10] Site web : http://ts5ri-voip-pfe.fr.gd/Protocoles-de-transport.htm

[11] Site web : http://wiki.wireshark.org/VoIP_calls

[12] F. Fela , V. Romain « Asterisk ». Dakar Regulatory Challenges of VoIP Africa, 2006.

[13] Site web : http://support.esi-stech.com/index.php?/Knowledgebase/Article/View/148/0/counterpath-x-lite-configuration

[13] J.Van Magglen, L. Madsen & J. Smith Foreword by M. Spencer « Asterisk- The Future of Telephony». O´Reilly, 2nd Ed, 2007.

[14] D. Endler et M. Collier « Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions ». McGraw-Hill/Osborne, 2007.

[15] « Hakin9 Sécurité pour le système Voice over «IP – protocoles SIP et RTP » Tobias Glemser, Reto Lorenz – 2005.

[16] O.Dabbebi, « Gestion des risques dans les infrastructures VoIP ». Thése Du Doctorat de l'Université de Lorraine, 2013.

[17] R. Bouzaida, « Etude et mise en place d'une solution VoIP sécurisée ». Mémoire de projet de fin d'études, 2011.