Faculté des Nouvelles Technologies de l'Information et la Communication
Département de l'informatique et Technologies de l'information

Travail présenté par: Hamed Hanane & Mezouar Asma Nesrine.
Encadré par: Khaldi Amine.

Réalisation d'une application VOIP (Voice Over Internet Protocole) chiffrée par VPN(virtual Privat Network)

1 Résumé :

La téléphonie sur IP est une technologie de communication importante et un systèmes de transmission de l'information de plus en plus utilisés de nos jours. La téléphonie sur IP (ou VoIP pour Voix sur IP) est un mode de téléphonie utilisant le protocole de télécommunications créé pour Internet (IP pour Internet Protocol). La voix est numérisée puis acheminée sous forme de paquets comme n'importe quelles données. L'objectif principal de notre travail est de concevoir une application de communication qui permettra l'échange sécurisé des données à travers l'établissement d'un tunnel virtuel sur un réseau publique. Les données seront chiffrées puis transmissent sur un réseau publique comme internet.

Mots clés : VOIP, VPN, chiffrement , échange de clés. AES, Diffie-Hellman

2 Introduction :

De nos jours les données sont transitées sur le réseau internet et ceux a travers le monde entier ce qui implique que la sécurisation des échanges est primordiale. Les VPN ont commencé à être mis en place pour répondre à ce type de problématique.

Dans notre travail nous allons sécuriser une communication VOIP entre deux hôtes distants. Cette sécurité apporté sera réaliser grâce au chiffrement des données via l'algorithme AES ce qui rendra les données inintelligible pour un tiers.

Notre travail est scindé en quatres chapitres:

Le premier chapitre est dédié à la présentation de la VOIP ainsi que la TOIP. Nous détaillerons ainsi les techniques de transmission de la voix en mode paquets, les équipements de communication, les protocoles utilisés ainsi que la sécurisation de la TOIP.

Dans le deuxième chapitre nous présenterons la cryptographie symétrique et asymétrique ainsi que les fonctions de hachage, la génération des clés et la signature numérique

Le Troisième chapitres présente les VPN, leur principe de fonctionnement, les protocoles utilisés pour réaliser une connexion VPN, ainsi qu'une comparaison des différents protocoles.

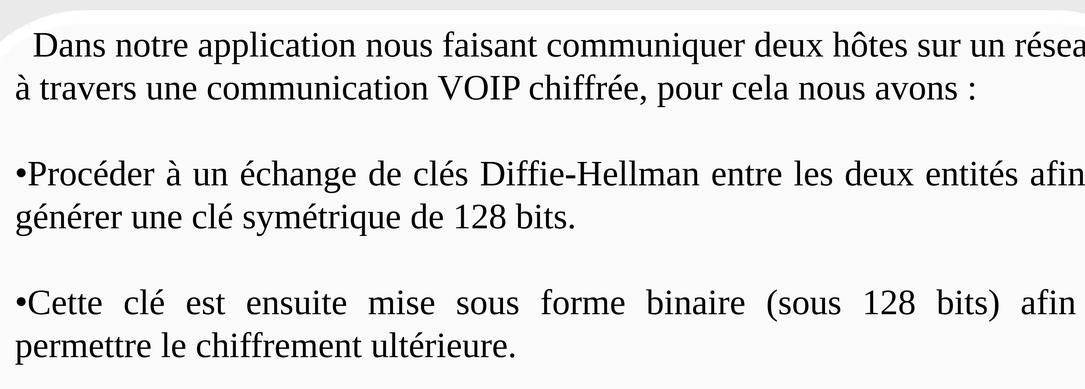
Dans le quatrième et dernier chapitre nous présenterons notre approche pour sécuriser une communication de bout en bout en chiffrant les données transmises par un chiffrement symétrique et ceux après une génération asymétrique de la clé.

3 Méthode :

•Langage utilisé : Afin d'implémenté notre application nous avons opté pour le langage JAVA sous l'environnement NetBeans

•L'échange de clés symétriques servant au chiffrement sera réalisé via l'algorithme de Diffie-Hellman qui permet un échange sécurisé des données

•Pour le chiffrement des données l'algorithme symétrique AES est appliqué en utilisant une clé de 128 bits



Processus de chiffrement de la VOIX

4 Résultats :

Dans notre application nous faisant communiquer deux hôtes sur un réseau à travers une communication VOIP chiffrée, pour cela nous avons :

•Procéder à un échange de clés Diffie-Hellman entre les deux entités afin de générer une clé symétrique de 128 bits.

•Cette clé est ensuite mise sous forme binaire (sous 128 bits) afin de permettre le chiffrement ultérieure.

•Apres établissement de la connexion et génération des clés, le flux vocal acquis est mis sous forme de paquet transporté par le protocole UDP.

•Chaque flux informationnel vocal est chiffré via l'algorithme AES avec la clé généré dans l'étape précédente et est transmis au destinataire.

•Chaque destinataire est apte à déchiffrer le flux réceptionné grâce à la clé généré durant la phase de connexion.

5 Conclusions:

Ce travail a pour but de créer une application VOIP chiffré entre deux hôtes distants au plus, à l'intérêt de la qualité et de fiabilité.

6 Bibliographie:

[1] : La Qualité de Service le la Voix sur IP Principes et Assurance : <http://wallu.pagesperso-orange.fr/VoIP.pdf >

[2]: Renaud Dumont, Cryptographie et Sécurité informatique INFO0045-2,2009 – 2010, R. Dumont - Notes provisoires Université de Liège.

[3] : RÉSEAU PRIVÉ VIRTUEL VPN : < http://www.frameip.com/vpn/>