

République Algérienne Démocratique et Populaire
Ministère de l'enseignement Supérieur et de la Recherche
Scientifique

Centre de Recherche sur l'Information Scientifique et
Technique

MEMOIRE POUR L'OBTENTION DU DIPLOME DE POST
GRADUATION SPECIALISEE EN SECURITE INFORMATIQUE

THEME

**ETUDE DE LA SECURITE SUR LA VOIX IP
(VoIP)**

Présenté par :

Mr CHAOUCHI ABDELKADER

Melle HAMED CHEIKH FETHIA

Encadré par :

Dr. TANDJAOUI DJAMEL

MEMBRES DU JURY:

DR. NOUALI OMAR

Président

Dr. MEZIANE ABDELKRIM

Mmembre

Dr. KHELLADI LYES

Membre

CERIST 2008

Remerciements

En premier lieu, nous remercions le DIEU, le tout puissant pour son aide et soutien. Nous remercions le professeur BADACHE Nadjib Directeur du CERIST de nous avoir accueilli au sein de son établissement pour suivre cette formation.

Merci à notre encadreur monsieur TANDJAOUI Djamel , qui nous a aidé à réaliser ce modeste travail, merci pour ses connaissances dans le domaine des réseaux informatiques et aussi pour ses idées qui nous ont permis de faire avancer en particulier l'aspect méthodologique.

Un grand merci pour Dr NOUALI Omar d'avoir accepté de présider ce jury.

Un merci tout particulier aux membres du jury qui ont accepté de juger notre travail et nous honorer par leur présence.

Un grand merci à nos collègues de travail et particulièrement aux responsables qui nous ont donné le temps et les moyens nécessaires pour bénéficier de cette formation.

Merci à tous les enseignants de la PGS Sécurité informatique qui nous ont aidé à acquérir énormément de connaissances dans le domaine de la sécurité informatique. .

Un merci à tous nos collègues de la PGS sécurité informatique.

Merci à tout le personnel du service de la formation pour son soutien particulier durant la période de nos études.

| | |
|--------------------|---|
| Introduction | 2 |
|--------------------|---|

CHAPITRE 1 : GENERALITES SUR LA VOIX SUR IP(VoIP)

| | |
|--|---|
| 1.1 La Voix sur IP..... | 4 |
| 1.2 Architecture VoIP..... | 4 |
| 1.3 Fonctionnement | 6 |
| 1.3.1 Acquisition du signal..... | 6 |
| 1.3.2 Numérisation | 6 |
| 1.3.3 Compression..... | 7 |
| 1.3.4 Habillage des en-têtes..... | 7 |
| 1.3.4.1 IP | 7 |
| 1.3.4.2 UDP | 7 |
| 1.3.4 Emission et transport..... | 7 |
| 1.3.5 Réception | 8 |
| 1.3.6 Conversion numérique analogique | 8 |
| 1.3.7 Restitution..... | 8 |
| 1.4 Types de la VoIP | 8 |
| 1.4.1 De PC à PC..... | 8 |
| 1.4.2 De PC à téléphone (ou vice-versa)..... | 8 |
| 1.4.3 De téléphone à téléphone | 8 |
| 1.5 Avantages..... | 8 |
| 1.6 Inconvénients..... | 9 |

CHAPITRE 2 : PROTOCOLES DE LA VOIX SUR IP(VOIP)

| | |
|---|----|
| 2.1 Protocoles de la VoIP | 11 |
| 2.1.1 Protocoles de signalisation | 11 |
| 2.1.1.1 Protocole H.323..... | 11 |
| 2.1.1.1.1 Architecture H.323 | 12 |
| 2.1.1.1.2 Principaux acteurs du protocole H.323 | 12 |
| 2.1.1.1.3 Protocoles constituant le protocole H.323 | 13 |
| 2.1.1.1.4 H323 dans le modèle OSI..... | 14 |
| 2.1.1.1.5 Etapes d'une communication H.323..... | 14 |
| 2.1.1.1.6 Avantages et inconvénients | 14 |
| 2.1.1.2 Protocole SIP..... | 15 |
| 2.1.1.2.1 Fonctionnement | 15 |
| 2.1.1.2.2 Architecture SIP | 17 |
| 2.1.1.2.3 Principaux acteurs du protocole SIP..... | 17 |
| 2.1.1.2.3.1 UAS (User Agent Server)..... | 17 |
| 2.1.1.2.3.2 U.A.C (User Agent Client)..... | 17 |
| 2.1.1.2.3.3 RS (Redirect Server)..... | 18 |
| 2.1.1.2.4 Sécurité et Authentification..... | 19 |
| 2.1.1.2.5 Avantages du protocole SIP | 19 |
| 2.1.1.2.6 Comparaison avec H323..... | 20 |
| 2.1.2 Protocoles de transport | 20 |
| 2.1.2.1 RTP (Real Time Protocol)..... | 20 |
| 2.1.2.1.1 Les fonctions de RTP | 21 |
| 2.1.2.1.2 Entête RTP | 22 |
| 2.1.2.2 RTCP (Real Time)..... | 23 |
| 2.1.2.2.1 Les fonctions de RTCP..... | 23 |
| 2.1.2.2.2 Entête RTCP | 24 |
| 2.1.3 Conclusion..... | 25 |

CHAPITRE 3 : securite de la voix sur IP (VoIP)

| | |
|---|----|
| 3.1 Les attaques sur les VoIP | 27 |
| 3.1.1 Attaques sur les couches basses | 27 |
| 3.1.1.1 ARP Spoofing..... | 27 |
| 3.1.1.2 ARP Cache Poisoning | 28 |
| 3.1.1.3 ARP MITM:Main In the Middle | 28 |
| 3.1.1.4 Le Déni de Service | 29 |
| 3.1.2 Attaques profitant des vulnérabilités des protocoles | 29 |
| 3.1.2.1 Attaques liées aux protocoles SIP | 29 |
| 3.1.2.1.1 Déni de service(DOS :Denial of service) | 29 |
| 3.1.2.1.1.1 DoS en utilisant les messages de requête SIP..... | 30 |
| 3.1.2.1.1.2 DoS en utilisant les messages de requête SIP BYE..... | 30 |
| 3.1.2.1.1.3 DoS en utilisant les messages de requête SIP Failure(4xx)..... | 30 |
| 3.1.2.1.2 Suivre des appel(1)..... | 30 |
| 3.1.2.1.3 Re-Invite/Répétition de session « Mid Session tricks » | 31 |
| 3.1.2.1.4 Inondation du serveur proxy..... | 31 |
| 3.1.2.1.5 Débordement de la table des enregistrements | 31 |
| 3.1.2.2 Attaques liées aux protocoles RTP..... | 31 |
| 3.1.2.2.1 Perte de performances Qos en réutilisant la SRRC de RTP | 31 |
| 3.1.2.2.2 Injection de paquets RTP..... | 31 |
| 3.1.2.2.3 Modification du codec audio | 32 |
| 3.1.2.2.4 Rendre le flux audio inaudible | 32 |
| 3.1.2.2.5 Ecoute clandestine physique..... | 32 |
| 3.1.2.2.6 Suivre des appels | 32 |
| 3.1.2.2.7 Détournement d'appel à l'aide du serveur registrar(1)..... | 33 |
| 3.1.2.2.8 Détournement d'appel à l'aide du serveur registrar(2)..... | 33 |
| 3.1.2.2.9 Détournement de l'enregistrement en façonnant des messages SIP REGISTER..... | 33 |
| 3.1.2.2.10 Détournement d'enregistrement | 33 |
| 3.1.2.2.11 Redirection d'appel en utilisant des messages de réponse du type 301/302 | 34 |
| 3.1.2.2.12 Redirection d'appel en utilisant des messages de réponse du type 305 | 34 |
| 3.1.2.2.13 Masquage d'appel..... | 34 |
| 3.1.2.2.14 Tromper la taxation | 34 |
| 3.1.2.2.15 Vol de service en utilisant les accréditations de l'utilisateur légitime..... | 34 |
| 3.1.2.2.16 Appel spam..... | 35 |
| 3.1.2.2.17 IM (Messagerie instantanée) spam..... | 35 |
| 3.1.2.2.18 Se faire passer pour un client..... | 35 |
| 3.1.3 Attaques sur les protocoles secondaires | 35 |
| 3.1.3.1 DNS Spoofing | 35 |
| 3.1.3.2 DNS cache poisoning | 36 |
| 3.2 Solutions VoIP | 36 |
| 3.2.1 Sécurité de base..... | 36 |
| 3.2.1.1 Mise à jour du software (IPBX, hardphone et softphone)..... | 36 |
| 3.2.1.2 Verrouillage de la configuration (hardphone/softphone) | 37 |
| 3.2.2 Séparation des équipements DATA et VoIP | 37 |
| 3.2.2.1 Séparation au niveau IP (layer 3) | 37 |
| 3.2.2.2 Séparation grâce aux VLAN (layer 2)..... | 37 |
| 3.2.2.3 Filtrage Inter-VLAN..... | 37 |
| 3.2.2.4 Sécuriser l'accès aux ports des switches (ACL,...)..... | 38 |
| 3.2.2.5 Placer les services convergés dans une DMZ..... | 38 |
| 3.2.3 Authentification..... | 38 |
| 3.2.3.1 Authentification HTTP Digest des messages SIP | 38 |
| 3.2.3.2 Authentification mutuelle..... | 38 |
| 3.2.4 Chiffrement | 39 |
| 3.2.4.1 Chiffrement du flux de signalisation : SIPS,..... | 39 |

| | | |
|---------|--|----|
| 3.2.4.2 | Chiffrement du flux média : SRTP..... | 39 |
| 3.2.4.3 | Chiffrement avec IPSec (ou autre technologie VPN)..... | 40 |
| 3.3 | Matrice attaques et solutions | 40 |

CHAPITRE 4 : DEPLOIEMENT DE LA SOLUTION

| | | |
|-----------|--|----|
| 4.1 | Scénario proposé | 43 |
| 4.2 | Solution proposé..... | 43 |
| 4.2.1 | Interconnexion Alger-Oran | 44 |
| 4.2.2 | Interconnexion Alger-Annaba | 44 |
| 4.3 | Le Protocole IPSec | 45 |
| 4.3.1 | Définition d'IPSec..... | 45 |
| 4.3.2 | Les services de sécurité fournis par IPSec | 45 |
| 4.3.2.1 | Confidentialité des données..... | 45 |
| 4.3.2.2 | Authenticité des données..... | 45 |
| 4.3.2.3 | Intégrité | 46 |
| 4.3.2.4 | Protection contre le rejeu..... | 46 |
| 4.3.3 | Architecture d'IPSec | 46 |
| 4.3.3.1 | AH (Authentication Header | 47 |
| 4.3.3.1.1 | Calcul de l'entête d'authentification | 48 |
| 4.3.3.1.2 | Modes de fonctionnement | 48 |
| a) | Mode transport | 48 |
| b) | Mode tunnel | 49 |
| 4.3.3.2 | Encapsulation Security Payload (ESP)..... | 49 |
| 4.3.3.2.1 | Modes de fonctionnement | 50 |
| a) | Mode transport | 50 |
| b) | Mode tunnel | 51 |
| 4.3.4 | Gestion des clés..... | 51 |
| Etape 1 | | 52 |
| a) | Mode principal | 52 |
| b) | Mode agressif..... | 52 |
| Etape 2 | | 52 |
| a) | Mode Rapide | 52 |
| b) | mode nouveau groupe | 52 |
| 4.3.4.1 | Infrastructures à clés publiques | 52 |
| 4.3.5 | Les associations de sécurité (SA) | 53 |
| 4.3.6 | Politique de sécurité | 53 |
| 4.3.6.1 | Principe de fonctionnement..... | 54 |
| a) | Trafic entrant (déchiffrement du bloc entrant) | 54 |
| b) | Trafic sortant (chiffrement du bloc sortant) | 55 |
| 4.3.7 | Déploiement de la solution..... | 55 |
| 4.3.7.1 | Déploiement d'IPSec avec Windows 2000 Server..... | 56 |
| 4.3.7.1.1 | Stratégies IPSec | 56 |
| 4.3.7.1.2 | Mise en place de la stratégie IPSec | 56 |
| 4.3.7.1.3 | Stratégies IPSec prédéfinies | 57 |
| a) | Client en réponse seule..... | 57 |
| b) | Serveur (demandez la sécurité)..... | 57 |
| c) | Sécuriser le serveur (nécessite la sécurité)..... | 58 |
| 4.3.7.1.4 | Test de fonctionnement | 61 |
| 4.3.7.2 | Déploiement d'IPSec Routeur Cisco 2600..... | 61 |
| 4.3.7.2.1 | Etapes de la Configuration | 62 |
| Etape 1 | | 62 |
| Etape 2 | | 62 |
| Etape3 | | 62 |
| 4.3.7.2.2 | Description des étapes de configurations | 63 |

| | |
|--|-----------|
| a) Sur le routeur de la Direction Générale (Alger) | 63 |
| b) Sur le routeur du Site d'Oran | 63 |
| 4.3.7.3 Déploiement d'IPSec sous Linux | 64 |
| Etape 1 : le téléchargement et l'installation de FreeS/WAN | 65 |
| Etape2 : génération des clés | 65 |
| Étape 3 : L'échange des clés | 65 |
| Etape 4 : le test de la configuration | 66 |
| 4.4 Conclusion..... | 66 |
| Conclusion Générale | 68 |
| Bibliographie..... | 70 |

Listes des figures

| | |
|--|----|
| Fig.1.1 : Architecture générale de la VoIP | 4 |
| Fig 1.2 : Etapes de fonctionnement de la VoIP | 6 |
| Fig. 2.1 : Architecture H.323 | 12 |
| Fig 2.2 : Protocole H.323 dans le modèle OSI | 14 |
| Fig. 2.3 : Architecture SIP | 17 |
| Fig. 2.4 : Exemple d'établissement d'une session SIP | 18 |
| Fig. 2.5 : Entête RTP | 22 |
| Fig. 2.6 : Entête RTCP | 24 |
| Fig. 4.1 : Réseau de l'entreprise propose | 44 |
| Fig. 4.2 : Interconnexion Alger-Oran | 45 |
| Fig. 4.3 : Interconnexion Alger-Annaba | 45 |
| Fig. 4.4 : IPSec dans le modèle OSI | 46 |
| Fig. 4.5 : Entête d'authentification IPSec | 47 |
| Fig. 4.6 : Service apporté en mode transport après utilisation de AH | 48 |
| Fig. 4.7 : Service apporté en mode tunnel après utilisation de AH | 49 |
| Fig. 4.8 : Encapsulation Security Payload | 49 |
| Fig. 4.9 : Service apporté en mode transport après utilisation de ESP | 50 |
| Fig. 4.10: Service apporté en mode tunnel après utilisation de ESP | 51 |
| Fig.4.11 : Composants d'IPSec et actions à l'émission de données | 54 |
| Fig.4.12 : Création de la stratégie de sécurité | 56 |
| Fig.4.13 : Sélection de l'emplacement où s'applique la stratégie de sécurité | 57 |
| Fig.4.14 : Les stratégies prédéfinis d'IPSec | 58 |
| Fig.4.15 : Attribution d'un nom à la politique de sécurité | 58 |
| Fig.4.16 : Configuration de la méthode d'authentification | 59 |
| Fig.4.17 : Propriétés de stratégie de sécurité | 59 |
| Fig.4.18 : Application des filtres | 60 |
| Fig.4.19 : Méthodes de sécurité d'échange de clés | 60 |
| Fig.4.20 : Attribution de la politique de sécurité | 61 |
| Fig.4.21 : Test du fonctionnement de la stratégie de sécurité | 61 |
| Fig.4.22 : Déploiement de la solution avec Routeur Cisco 2600 | 62 |
| Fig.4.23 : Format du fichier /etc/ipsec.conf | 65 |
| Fig.4.24 : Génération des clés | 65 |
| Fig 4.25: Le démarrage de IPSEC | 66 |