

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediene



Faculté d'Electronique et Informatique
Département de Télécommunications

Mémoire de MASTER
Domaine : Sciences et Technologie
Filière : Télécommunications
Spécialité : Télécommunication, Réseau & Multimédia

THEME

Sécurité du protocole SIP dans les réseaux
mesh sans fil

Proposé et dirigé par : Mr. Nadir BOUCHAMA

Présenté par :
YENNOUNE Walid
DAI Younes

Soutenu le/../....

Devant le jury composé de :

Président : Mr. Slimane MEKAOUI

Examineur : Mr. Abdellah SKOUDARLI

Promoteur : Mr. Nadir BOUCHAMA

Co-promoteur : Mr. S Hamrioui

Promotion: 2015-2016

Remerciements

Au terme de ce travail, nous tenons à remercier en particulier notre encadreur « Mr .BOUCHAMA Nadir » qui nous a proposé ce sujet. Nous lui adressons nos sincères remerciements pour ses conseils précieux qui nous ont été de grande utilité tout au de notre travail.

Nos remerciements les plus vifs s'adressent aussi à monsieur le président et les membres de jury qui ont accepté d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les enseignants qui ont collaboré à notre formation de Master.

Enfin nous remercions tous ceux qui ont contribué de pré ou de loin à la réalisation de ce travail.

Dédicaces

Nous dédions ce modeste travail :

À nos très chers parents.

À nos frères et sœurs.

À nos grands-parents et toutes nos familles.

À tous ceux qui nous aidions durant nos études.

*À tous nos **enseignants** qui nous donnent le maximum durant nos études.*

*À tous nos **amis(es)** : de la vie et des études.*

À tous ceux qui nous aidions durant nos vies universitaires.

À tous la promotion TRM.

YENNOUNE Walid - DAI Younes

Liste des figures

Figure 1.1. Maillage total	4
Figure 1.2. Maillage partiel	5
Figure 1.3. Architecture clients	5
Figure 1.4. Architecture Backbone	6
Figure 1.5. Architecture hybride	7
Figure 1.6. Classification des protocoles de routage dans les Mesh	9
Figure 1.7. Fonctionnement du routage OLSR	10
Figure 2.1. Architecture générale de la VoIP	14
Figure 2.2. Passage du signal analogique au signal numérique	14
Figure 2.3. La pile protocolaire de SIP	15
Figure 2.4. Composants d'une architecture SIP	17
Figure 2.5. Format d'un message SIP	17
Figure 2.6. Le processus d'enregistrement [17]	20
Figure 2.7. Etablissement et terminaison d'une session SIP [20]	20
Figure 3.1. classification des attaques SIP	25
Figure 3.2. Attaque par le BYE	26
Figure 3.3. Attaque par le CANCEL.....	26
Figure 3.4. Attaque sur le REGISTER	27
Figure 3.5. DoS Bulk-REGISTER.....	27
Figure 3.6. DoS Invite-Flood	28
Figure 3.7. Exemple de détournement d'appel " Man in the middle"	29
Figure 3.8. Classification des attaques de sécurité pour différentes couches	30
Figure 3.9. Mécanisme de sécurité SIP	31
Figure 3.10. Enregistrement et authentification HTTP Digest dans un contexte SIP.....	32
Figure 4.1. Architecture du réseau WMN.....	37
Figure 4.2. Configuration de base du routeur.....	38
Figure 4.3. Configuration de routage (protocole OLSR).....	38
Figure 4.4. Configuration basique de l'interface de Backbone	39
Figure 4.5. Configuration d'adressage du point d'accès	40
Figure 4.6. Configuration de routage.....	40
Figure 4.7. Affectation de mode AP (point d'accès)	41
Figure 4.8. Initialisation des partitions	42

Figure 4.9. Configuration de l'adressage IP pour le serveur Asterisk	42
Figure 4.10. Configuration du mot de passe pour le serveur Asterisk.....	43
Figure 4.11. Configuration des clients	43
Figure 4.12. Configuration des extensions	44
Figure 4.13. Configuration du compte du client « 3001 »	45
Figure 4.14. Crack de la clé WEP.....	45
Figure 4.15. Intrusion du Hacker	46
Figure 4.16. Scan du réseau	47
Figure 4.17. Attaque MITM	47
Figure 4.18. Table ARP avant l'attaque	48
Figure 4.19. Table ARP après l'attaque	48
Figure 4.20. L'interface principale de Wireshark	49
Figure 4.21. Analyse des paquets RTP capturés	49
Figure 4.22. Choisir une conversation à écouter	49
Figure 4.23. Ecoute d'une conversation enregistrée. entre 2 clients	50
Figure 4.24. Ajout d'un client pour le softphone Bl..ink	51
Figure 4.25. Configuration du client avec le certifi..cat et clé de chiffrement	52
Figure 4.26. Appel chiffré utilise TLS	52
Figure 4.27. Echanges TLS pour SIP	53
Figure 4.28. Sécurisation du flux RTP	54
Figure 4.29. Appel sécurisé avec TLS et SRTP	55
Figure 4.30. DoS sur un client Blink	59
Figure 4.31. Listes des adresses IP bloquées sur fa..il2ban	62

Liste des tableaux

Tableau 1.1. La différence entre un réseau mesh et un réseau ad-hoc	8
Tableau 2.1. Les requêtes SIP.....	18
Tableau 2.2. Les réponses SIP.....	18
Tableau 2.3. Délai d'acheminement.....	22
Tableau 4.1. Tableau récapitulatif des attaques réalisées	63

Sommaire

Liste des figures

Liste des tableaux

Introduction générale	1
Chapitre 1 : Les réseaux mesh sans fil	3
1 Introduction.....	3
2 Définition d'un réseau Mesh	3
3 Les équipements d'un réseau Mesh	3
4 Classification des WMNs	4
4.1 Selon le type de maillage	4
4.1.1 Maillage total.....	4
4.1.2 Maillage partiel	4
4.2 Selon l'architecture	5
4.2.1 Architecture clients.....	5
4.2.2 Architecture Backbone	6
4.2.3 Architecture hybride	6
5 Avantage des WMNs	7
6 La différence entre un réseau WMN et un réseau Ad-hoc	7
7 Domaines d'application	8
8 Protocoles de routage	9
8.1 Les protocoles de routage proactifs	9
8.1.1 OLSR (Optimized Link State Routing)	10
8.2 Les protocoles de routage réactifs	11
8.3 Les protocoles de routage hybrides	11
9 Défis et problèmes liés aux WMN	11
9.1 Interférences et collisions	11
9.2 Qualité de service	12
9.3 Sécurité.....	12
9.4 Passage à l'échelle	12

10 Conclusion	12
Chapitre 2 : Généralités sur la VoIP.....	13
1 Introduction	13
2 Définition	13
3 Principe de fonctionnement	13
4 Architecture de la VoIP	14
5 Les Protocoles de la VoIP	15
5.1 Protocole H.323	15
5.2 Protocole SIP	15
5.2.1 Entités SIP	16
5.2.1.1 L'agent utilisateur (UA, User Agent)	16
5.2.1.2 L'enregistreur (Registrar)	16
5.2.1.3 Le serveur proxy (Proxy Server)	16
5.2.1.4 Le serveur de redirection (Redirect server)	16
5.2.1.5 Le serveur de localisation (Location Server)	16
5.2.2 Format des adresses SIP	17
5.2.3 Syntaxe de message	17
5.2.3.1 Méthode du message	18
5.2.3.2 L'entête d'un message SIP	19
5.2.3.3 Corps du message	19
5.2.4 Fonctionnement de SIP	19
5.2.4.1 Enregistrement	19
5.2.4.2 Etablissement et terminaison d'une session SIP	20
5.2.4.2.1 Etablissement d'une session	20
5.2.4.2.2 Terminaison d'une session	21
6 Protocole du transport VoIP	21
6.1 Protocole RTP	21
6.2 Protocole RTCP	22
7 Les contraintes de la VoIP sur IP	22
7.1 Qualité du codage	22

7.2	Délai d'acheminement (latence)	22
7.3	Gigue (JITTER)	23
7.4	Perte des paquets	23
8	La VoIP sur les WMNs	23
9	Conclusion	23
	Chapitre 3 : Sécurité du protocole SIP.....	24
1	Introduction	24
2	Les Besoins de sécurité	24
3	Les Attaques sur les réseaux SIP	25
3.1	Quelques Attaques contre le protocole SIP	25
3.1.1	Attaques DoS (denial of service)	25
3.1.1.1	L'attaque par la méthode du BYE	26
3.1.1.2	L'attaque par la méthode du CANCEL	26
3.1.1.3	L'attaque par la méthode du Désenregistrement REGISTER	27
3.1.1.4	L'attaque par la méthode Bulk-REGISTER	27
3.1.1.5	L'attaque par la méthode INVITE flood	28
3.1.2	Détournement d'appel (call hijacking)	28
3.1.3	Attaque par écoute clandestine (Eavesdropping)	29
3.1.4	Attaque d'usurpation d'identité	29
3.2	Les attaques de sécurité réseau mesh	30
3.2.1	Attaque de brouillage (Jammingattack)	31
3.2.2	Attaque trou noir (Black-hole)	31
3.2.3	Attaque de trou-gris (Gray-hole)	31
3.2.4	Attaque de trou-ver (Worm-holeAttack)	31
4	Les Mécanismes de sécurité SIP.....	31
4.1	La sécurisation de la signalisation	32
4.1.1	L'authentification http	32
4.1.2	Secure MIME (S/MIME)	33
4.1.3	Transport Layer Security (TLS).....	33
4.1.4	IP security (IPsec)	34

5	Les limites des solutions actuelles	34
6	Conclusion	35
Chapitre 4 : Déploiement et sécurisation d'une plateforme VoIP dans un réseau mesh.....		36
1	Introduction	36
2	Architecture du réseau WMN	36
3	Configuration des routeurs mesh et des points d'accès	37
3.1	Configuration des routeurs	38
3.2	Configuration des points d'accès	39
4	Installation et configuration d'Asterisk	41
4.1	Installation d'Asterisk	42
4.2	Configuration d'Asterisk	43
4.2.1	Configuration des comptes utilisateurs	43
4.2.2	Configuration des extensions	44
5	Installation du softphone Blink	44
6	Attaques Simulées	45
6.1	Attaque Eavesdropping	46
6.2	Attaque usurpation d'identité	55
6.3	Attaque DOS de type inviteflood	57
7	Conclusion	63
	Conclusion générale	64
Bibliographie		
Liste des acronymes		
Annexe I : Le protocole SRTP		