

Université des Sciences et de la Technologie Houari Boumediene

Faculté d'Electronique et Informatique

Département d'Informatique

THÈSE

Présentée pour l'obtention du grade

Magister

En : INFORMATIQUE

Spécialité : Programmation et Systèmes

Intitulée

La sécurité dans le protocole Mobile IP:
*Un nouveau schéma d'authentification pour l'environnement
Mobile IP*

Manel CHENAIT

Jury :

Mr. A. AISSANI	Professeur, USTHB,	Président
Mme Z. ALIMAZIGHI	Professeur, USTHB,	Examineur
Mr S. LARABI	Maître de conférences, USTHB,	Examineur
Mr. N. BADACHE	Professeur, USTHB,	Rapporteur
Mr. D. TANDJAOUI	Attaché de recherche, CERIST,	Co-rapporteur

Sommaire

Introduction générale.....	5
----------------------------	---

CHAPITRE I: Généralités sur les environnements mobiles.

1.1 Introduction.....	7
1.2 Architecture d'un système distribué avec sites mobiles.....	7
1.3 Modes de fonctionnement des mobiles.....	8
1.3.1 Mode connecté.....	8
1.3.2 Mode partiellement connecté.....	9
1.3.3 Mode veille.....	9
1.3.4 Mode déconnecté.....	9
1.4 Les types de réseaux sans fil.....	9
1.5 Les caractéristiques des environnements mobiles.....	10
1.5.1 Les connexions sans fil.....	10
1.5.1.1 Les déconnexions.....	10
1.5.1.2 La faible largeur de la bande passante.....	11
1.5.1.3 L'hétérogénéité des réseaux.....	11
1.5.1.4 Les risques de sécurité.....	12
1.5.2 La mobilité.....	12
1.5.2.1 La migration d'adresse et la gestion de localisation.....	12
1.5.2.2 Les informations de localisation.....	13
1.6 Conclusion.....	13

CHAPITRE II: La mobilité IP.

2.1 Introduction.....	14
2.2 Le protocole IP.....	15
2.2.1 IPv6: Le nouveau protocole et ses solutions.....	15
2.2.2 Le problème de la mobilité IP.....	16
2.3 Définitions.....	16
2.4 Le handoff dans l'environnement mobile.....	17
2.5 Le fonctionnement du protocole Mobile IPv4.....	19
2.5.1 La découverte des agents.....	19
2.5.2 L'enregistrement.....	19
2.5.3 Le tunneling.....	20
2.6 Le scénario de communication du Mobile IPv4.....	21
2.7 Optimisation de route dans Mobile IP de base.....	23
2.7.1 Le binding cache.....	23
2.7.2 Smooth handoff entre les foreign agents.....	24
2.7.3 Utilisation de tunnels spéciaux.....	24
2.8 Le protocole successeur: Mobile IPv6.....	25
2.9 Fonctionnalités requises.....	26

2.10 Le scénario de communication du Mobile IPv6.....	26
2.11 Limites de Mobile IP (Solution de micro mobilité).....	27
2.12 Conclusion	27

CHAPITRE III: La sécurité dans le protocole Mobile IP.

3.1 Introduction.....	29
3.2 Attaques dans le monde mobile.....	30
3.2.1 Attaques sur les machines mobiles	30
3.2.2 Attaques sur l'agent mère et les correspondants.....	30
3.2.3 Attaques sur le réseau visité.....	31
3.2.4 Attaques sur les autres machines de l'Internet.....	31
3.3 Les besoins de sécurité.....	32
3.3.1 L'authentification.....	32
3.3.2 L'intégrité.....	32
3.3.3 L'autorisation (control d'accès)	32
3.3.4 La confidentialité	32
3.3.5 La non-répudiation.....	32
3.3.6 La gestion des clés	33
3.4 Les schémas d'authentification proposés pour Mobile IP	33
3.4.1 L'authentification standard dans Mobile IP.....	33
3.4.2 L'authentification basée sur les clés publiques	35
3.4.3 L'authentification Mobile IP/AAA.....	36
3.5 Le protocole Diameter.....	38
3.5.1 Les acteurs de Diameter dans Mobile IP.....	38
3.5.2 Le fonctionnement de Diameter dans Mobile IPv4.....	40
3.6 Conclusion.....	43

CHAPITRE IV: Un nouveau schéma d'authentification pour Mobile IP.

4.1 Introduction.....	45
4.2 Le problème de la ré-authentification locale dans le schéma Mobile IP/AAA	46
4.3 Présentation générale du protocole (Local MIP/AAA)	47
4.3.1 La certification du serveur local.....	48
4.3.2 La génération et la distribution des nouvelles clés	49
4.4 Schéma descriptif de la proposition.....	49
4.4.1 Le handover de Type I (First Inter domain handover)	49
4.4.2 Le handover de Type II (Intra domain handover).....	52
4.4.3 Le handover de Type III (Inter foreign domain handover).....	54
4.5 Avantages et inconvénients de la solution	55
4.5.1 Avantages.....	55
4.5.2 Inconvénients.....	55
4.6 L'algorithme	56
4.7 Conclusion.....	60

CHAPITRE V: Démarche et résultats d'analyse.	
5.1 introduction	61
5.2 Délai d'authentification dans le schéma Mobile IP/AAA	61
5.2.1 Temps de transfert.....	61
5.2.2 Temps des opérations cryptographiques	63
5.2.3 Délai complet d'authentification.....	64
5.3 Délai d'authentification dans le schéma Local Mobile IP/AAA.....	65
5.3.1 Premier cas : handover de Type I.....	65
5.3.1.1 Temps de transfert du flux	65
5.3.1.2 Temps des opérations cryptographiques	66
5.3.1.3 Délai complet d'authentification	67
5.3.2 Deuxième cas : handover de Type III.....	68
5.3.2.1 Temps de transfert du flux	68
5.3.2.2 Temps des opérations cryptographiques	68
5.3.2.3 Délai complet d'authentification	69
5.3.3 Troisième cas : handover de Type II	69
5.3.3.1 Estimation du temps de génération/chiffrement des nouvelles clés	69
5.3.3.2 Temps de transfert de flux	71
5.3.3.3 Temps des opérations cryptographiques	71
5.3.3.4 Délai complet d'authentification.....	72
5.4 Tableau récapitulatif	73
5.5 Conclusion.....	74
Conclusion générale	76
Bibliographie.....	79