

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENNE



U.S.T.H.B

Faculté d'Electronique et d'Informatique
Département d'Informatique



Mémoire de Fin d'Etudes

Pour l'obtention du diplôme d'Ingénieur d'Etat en Informatique

Thème

***Etude et Implémentation d'un Schéma de Sécurisation
dans un Environnement de Micro-Mobilité***

Proposé par :

M^r TANDJAOUI DJAMEL

M^{elle} CHENAÏT MANEL

Présenté par :

M^r HEDJEM AMINE

M^r TAHRAOUI ABDELMOHCENE

Soutenu devant le Jury :

M^r A. AISSANI ***Président***

M^r K. BENABADJI ***Membre***

M^r A. ABDELLI ***Membre***

Organisme d'accueil : Centre de Recherche sur l'Information Scientifique et Technique
-Laboratoire des Logiciels de Base-

Promotion : 2004-2005 /N° 88

Sommaire

<i>Introduction générale</i>	1
 <i>Chapitre 1 : La Sécurité Informatique</i>	
1.1. Introduction.....	3
1.2. Les menaces contre le sécurité.....	4
1.2.1. Les menaces accidentelles.....	4
1.2.2. Les menaces intentionnelles.....	4
1.2.3. Exemples d'attaques.....	5
1.2.3.1. Attaques contre la communication.....	5
1.2.3.2. Attaques logicielles.....	6
1.2.3.3. Autres attaques.....	7
1.3. Les besoins de sécurité.....	7
1.3.1. La confidentialité.....	8
1.3.2. L'authentification.....	8
1.3.3. L'intégrité.....	8
1.3.4. La non-répudiation.....	8
1.3.5. La disponibilité.....	9
1.3.6. Le contrôle d'accès.....	9
1.4. Comment assurer les besoins de la sécurité informatique ?	9
1.5. La cryptographie.....	9
1.5.1. Définitions.....	9
1.5.2. Notions élémentaires.....	10
1.5.2.1. La cryptographie invulnérable.....	11
1.5.2.2. Types de cryptographie	11
1.6. Conclusion.....	19

Chapitre 2 : Les protocoles de Macro et de Micro-Mobilité

2.1. Introduction.....	20
2.2. Terminologie.....	21
2.3. Le protocole Mobile IP	21
2.3.1. Le Handoff.....	22
2.3.2. Mobile IP : Architecture de base.....	23
2.3.3. Les protocoles IP	24
2.3.3.1. Le protocole IPv4.....	24
2.3.3.2. Le protocole IPv6.....	24
2.3.4. Le protocole Mobile IPv4.....	25
2.3.5. L'optimisation de route dans Mobile IPv4.....	29
2.3.6. Le protocole Mobile IPv6.....	29
2.3.6.1. Fonctionnalités requises.....	30
2.3.6.2. La Communication dans Mobile IPv6.....	30
2.3.7. Les inconvénients du protocole Mobile IP.....	31
2.4. La Micro-Mobilité.....	32
2.4.1. Le protocole Cellular IP.....	33
2.4.1.1. Architecture de Cellular IP.....	33
2.4.1.2. Les entités architecturale.....	34
2.4.1.3. Les buts de conception du protocole Cellular IP.....	35
2.4.1.4. Le fonctionnement du protocole Cellular IP.....	35
2.4.2. Le protocole HAWAII.....	40
2.4.2.1. Architecture du réseau HAWAII.....	40
2.4.2.2. Le fonctionnement du protocole	40
2.4.2.3. Les mécanismes du Handover dans HAWAII.....	42
2.4.3. Le protocole Mobile IP Hiérarchique (HMIP).....	44
2.4.3.1. Architecture Hiérarchique	44
2.4.3.2. Le bi casting dans une architecture hiérarchique.....	45
2.4.3.3. Le fonctionnement du protocole HMIPv4.....	45
2.4.3.4. Le fonctionnement du protocole HMIPv6.....	46
2.5. Conclusion.....	47

Chapitre 3 : La Sécurité dans les protocoles de Macro et de Micro-Mobilité

3.1. Introduction.....	49
3.2. Les attaques dans le monde Mobile.....	50
3.2.1. Attaques sur les machines mobiles.....	50
3.2.2. Attaques sur l’agent mère et les correspondants.....	50
3.2.3. Attaques sur le réseau visité.....	51
3.2.4. Attaques sur les autres machines de l’Internet.....	51
3.3. La sécurité dans le protocole Mobile IP.....	51
3.3.1. L’authentification dans Mobile IP.....	51
3.3.2. Les solutions proposées pour sécuriser le protocole Mobile IP.....	52
3.3.2.1. L’authentification standard dans Mobile IP.....	52
3.3.2.2. L’authentification basée sur les clés publiques.....	53
3.3.2.3. L’authentification Mobile IP/AAA.....	54
3.4. La sécurité dans les protocoles de Micro-Mobilité.....	55
3.4.1. La sécurité dans le protocole Cellular IP.....	55
3.4.1.1. La sécurité standard dans le protocole Cellular IP.....	55
3.4.1.2. L’authentification à l’aide des chaînes de hachage (UOBT).....	57
3.4.2. La sécurité dans le protocole HAWAII.....	60
3.4.2.1. Quelques caractéristiques de la sécurité dans HAWAII.....	61
3.4.3. La sécurité dans le protocole Mobile IP Hiérarchique (HMIP).....	62
3.4.4. La Micro-Mobilité et la solution FATIMA.....	62
3.4.4.1. L’architecture FATIMA.....	62
3.4.4.2. Les entités du réseau FATIMA.....	62
3.4.4.3. L’aspect de sécurité.....	64
3.5. Conclusion.....	66

**Chapitre 4 : Secure CIP : Un nouveau schéma d’authentification
pour le protocole Cellular IP**

4.1. Introduction.....	67
4.2. Le problème de la ré-authentification locale dans Cellular IP.....	67

4.3. Présentation générale de « Secure CIP ».....	68
4.4. Le scénario Secure CIP.....	69
4.5. Secure CIP: Avantages et inconvénients.....	71
4.5.1. Avantages.....	71
4.5.2. Inconvénients.....	71
4.6. Algorithme.....	71
4.7. Conclusion.....	73

Chapitre 5 : Démarches et Résultats de Simulation

5.1. Introduction.....	74
5.2. Présentation du simulateur réseau NS-2.....	74
5.2.1. Architecture et Implémentation.....	75
5.2.2. Statistiques et visualisation.....	76
5.2.2.1. Système de suivi.....	76
5.2.2.2. The Network Animator (NAM).....	76
5.3. La version de NS-2 utilisée.....	77
5.4. L'environnement de notre simulation.....	77
5.5. Démarche de simulation.....	78
5.5.1. Scénario de simulation.....	78
5.5.2. Simulation du protocole Secure CIP.....	79
5.5.3. Résultats et interprétations.....	81
5.5.3.1. La perte de paquet.....	81
5.5.3.2. Délai de transmission.....	84
5.6. Conclusion.....	86

Conclusion générale.....	87
---------------------------------	-----------

Bibliographie.....	89
---------------------------	-----------

Résumé

Les réseaux IP ont été mis en place initialement par l'interconnexion d'hôtes fixes reliés par un réseau filaire, l'objectif était d'offrir une communication rapide à haut débit. De nos jours, on essaye de plus en plus de rendre ces équipements IP mobiles.

Dans ce processus, on sépare généralement la gestion de la mobilité en deux parties distinctes : macro et micro-mobilité, suivant l'échelle des mouvements des nœuds mobiles.

Cependant, le déplacement des nœuds mobiles hors de leurs réseaux d'origine peut être la source d'attaques mal intentionnées (vol de session, écoute passive,...). Il faut pouvoir assurer une bonne authentification du nœud mobile avant de lui permettre l'accès aux réseaux étrangers, et cela quelque soit son domaine d'origine.

Beaucoup de solutions ont été proposé pour l'amélioration de la qualité de service dans l'environnement mobile mais celles qui concernent la sécurité restent encore rares.

Ce mémoire présente un nouveau schéma d'authentification pour le protocole de micro-mobilité Cellular IP et qui propose des améliorations à l'ancien schéma standard. L'idée de base est la re-génération de nouvelles clés pour l'authentification locale.

Mots clés : la sécurité, l'authentification, la micro-mobilité, Cellular IP, HAWAII, HMIP.