

République Algérienne Démocratique et Populaire

Université des Sciences et de la Technologie Houari Boumediène

**USTHB**

Institut du Génie Electrique

Département d'informatique

*Mémoire de fin d'études  
pour l'obtention du titre d'ingénieur d'état  
en informatique*

Option: Software



**Thème**

**Agents Mobiles Anonymes**



membres du jury

N. Badache (président)

M. Benchaïba (examinateur)

S. Moussaoui (examinatrice)

Proposé et encadré par :

Mme S. Benmeziane

Attachée de recherche

LLB, CERIST

Présenté par :

Baghdad Larab et

Abdelhakim Zerhouni

Promotion 2003

N° 62/03

# Sommaire

Introduction générale .....	4
Organisation du mémoire .....	5
<b>CHAPITRE 1 : LES AGENTS MOBILES .....</b>	<b>6</b>
1.1 Introduction.....	7
1.2 Définition d'agent .....	7
1.3 Propriétés des Agents .....	7
1.4 Types d'Agents .....	8
1.5 Les Agents Mobiles.....	9
1.5.1 Définition .....	9
1.5.2 Origines.....	9
1.5.3 Avantages des Agents mobiles.....	10
1.5.3.1 Répartition dynamique de charge.....	10
1.5.3.2 Diminution du trafic réseau.....	10
1.5.3.3 Administration du système.....	11
1.5.4 Les principaux problèmes .....	11
1.5.4.1 La sécurité.....	11
1.5.4.2 L'interopérabilité.....	11
1.5.5 Propriétés des Agents mobiles .....	12
1.5.5.1 La Migration.....	12
1.5.5.2 L'acquisition des données .....	12
1.5.5.3 La Détermination de la route.....	12
1.5.5.4 La Communication.....	12
1.5.5.5 L'autorité.....	13
1.5.6 Domaines d'Applications des Agents mobiles.....	13
1.5.7 Présentation de plateformes d'agents mobiles .....	14
1.5.7.1 Sur Java.....	14
1.5.7.2 Autres environnements (Tcl, Python ..).....	15
1.6 Conclusion .....	15
<b>CHAPITRE 2 : LA SECURITE INFORMATIQUE : SERVICES ET MECANISMES .....</b>	<b>16</b>
2.1 Introduction.....	17
2.2 Services de Sécurité .....	17
2.2.1 La confidentialité .....	17
2.2.2 L'intégrité.....	17
2.2.3 La disponibilité de service.....	18
2.2.4 L'authentification.....	18
2.2.4.1 Authentification d'entités (entity authentication).....	18
2.2.4.2 Authentification de l'origine de données (data origin authentication) .....	18
2.2.5 La non répudiation .....	18
2.2.6 La non duplication.....	19
2.2.7 L'anonymat (d'entité ou d'origine de données) .....	19
2.3 Mécanismes de base.....	20
2.3.1 Les outils cryptographiques .....	20
2.3.1.1 Notions de bases.....	20
2.3.1.2 Cryptographie Symétrique .....	21
2.3.1.3 Cryptographie Asymétrique .....	22
2.3.1.4 Signature numérique .....	23
2.3.1.5 Comparaison des deux méthodes (symétrique vs. Asymétrique).....	25
2.3.2 Autres mécanismes de sécurité .....	25
2.3.2.1 Mécanismes de bourrage .....	25
2.3.2.2 Mécanismes de contrôle de routage.....	26
2.3.2.3 Mécanisme de notariation .....	26
2.3.3 Evaluation des menaces, risques et contre-mesures .....	26
Politique de sécurité .....	27
2.4 Conclusion .....	27
<b>CHAPITRE 3 : SECURITE DES AGENTS MOBILES .....</b>	<b>28</b>
3.1 Introduction.....	29
3.2 Les menaces de sécurité.....	29

3.2.1	Agent-à-Plateforme .....	30
3.2.1.1	Le déguisement (masquerading).....	30
3.2.1.2	Le déni de service.....	30
3.2.1.3	L'accès non autorisé.....	30
3.2.2	Agent-à-Agent.....	31
3.2.2.1	Le déguisement .....	31
3.2.2.2	Le déni de service.....	31
3.2.2.3	La répudiation .....	31
3.2.2.4	L'accès non autorisé.....	32
3.2.3	Plateforme-à-Agent .....	32
3.2.3.1	Le déguisement .....	32
3.2.3.2	Le déni de service.....	32
3.2.3.3	Écoute clandestine (eavesdropping).....	33
3.2.3.4	L'altération.....	33
3.2.4	D'autres-à-Plateforme d'agents .....	34
3.2.4.1	Le déguisement .....	34
3.2.4.2	L'accès non autorisé.....	34
3.2.4.3	Le déni de service.....	34
3.2.4.4	La duplication et le rejeu (Copy and replay).....	35
3.3	Services de Sécurité liés aux agents mobiles .....	35
3.3.1	La confidentialité .....	35
3.3.2	L'intégrité.....	36
3.3.3	La responsabilité (accountability) .....	37
3.3.4	La disponibilité .....	39
3.3.5	L'anonymat .....	40
3.4	Protection des Agents.....	40
3.4.2.1	Encapsulation Partielle du Résultat.....	41
3.4.2.2	Enregistrement Mutuel d'Itinéraire .....	41
3.4.2.3	Enregistrement de l'itinéraire avec réplique et vote.....	42
3.4.2.4	Traçage d'exécution.....	42
3.4.2.5	Génération de clé environnementale .....	43
3.4.2.6	Calcul avec des fonctions chiffrées.....	43
3.5	Conclusion .....	44
<b>CHAPITRE 4 : L'ANONYMAT DES AGENTS MOBILES.....</b>		<b>45</b>
4.1	Introduction.....	46
4.2	Définition de l'Anonymat .....	46
4.3	Caractéristiques de l'anonymat .....	46
4.4	Techniques de Base.....	47
4.4.1	Routerage Aléatoire (Randomized Routing).....	47
4.4.2	Adressages Explicites et Implicites .....	48
4.4.3	Renvoi à travers une Tierce de Confiance.....	48
4.4.4	Amélioration du TTP pour résister aux attaques .....	48
a.	Redéfinir la sémantique du protocole.....	48
b.	Casser le lien de Temps.....	48
c.	Casser le lien de Taille .....	48
d.	Casser le lien d'existence .....	49
4.4.5	Mixes de Chaum .....	49
4.4.6	Les Circuits virtuels .....	50
4.5	La signification des attaques .....	51
4.6	La signification de la défense.....	51
4.6.1	La signification de la défense.....	51
4.6.2	Conditions de sécurité garantissant l'anonymat .....	51
4.6.3	Une étude des schémas de protection pour garantir l'anonymat.....	52
4.7	Anonymat dans les systèmes d'agents mobiles .....	52
4.7.1	Solutions pour l'anonymat.....	52
4.7.1.1	Mixing.....	52
4.7.1.2	Signatures de groupe .....	52
4.7.1.3	Signature en aveugle .....	53
4.7.2	Les Agents anonymes .....	53
4.8	Conclusion .....	54

CHAPITRE 5 : CONCEPTION ET REALISATION D'AGENTS MOBILES ANONYMES .....	55
5.1 Introduction.....	56
5.2 Choix de la technique.....	56
5.3 Choix de la plateforme.....	56
5.4 La plateforme d'Agents Mobiles « Ajanta ».....	57
5.4.1 Introduction.....	57
5.4.2 Architecture du Système Ajanta.....	57
5.4.3 La classe Agent et ses primitives de programmation .....	60
5.4.3.1 Création et acheminement d'un agent.....	61
5.4.3.2 Actions d'arrivée et de départ.....	62
5.4.3.3 Migration de l'Agent.....	62
5.4.4 Architecture et sécurité du serveur d'agents .....	63
5.4.4.1 Protocole de Transfert d'Agent (ATP).....	64
5.4.4.2 Le Traitement d'Exception : Le Guardian .....	65
5.4.4.3 Le contrôle des Agents distants.....	65
5.4.4.4 Protection des Ressources du Serveur.....	66
5.4.4.5 Communication Inter-agents .....	67
5.4.5 Protection des Agents.....	68
5.4.5.1 Sécurité contre les attaques potentielles.....	68
5.4.5.2 Protection de l'état de l'agent.....	68
5.4.6 Itinéraires et modèles pour la migration d'agent.....	68
Applications à base d'agents.....	70
• Web Index Search Service .....	70
• Système Global d'Accès au Fichier (système à distance d'accès aux fichiers à base d'agents).....	70
• Un Système de Gestion de Calendrier .....	70
5.4.8 Conclusion .....	70
5.5 Conception, Implémentation et Tests.....	71
5.5.1 Introduction.....	71
5.5.2 Architecture Globale .....	71
5.5.2.1 Le module AnonAgent.....	71
5.5.2.2 Le serveur Mix .....	71
5.5.2.3 Le Name Registry .....	71
5.5.3 Interaction entre les composants du système.....	72
5.5.3.1 L'initialisation de l'agent (Mixing).....	72
5.5.3.2 La migration .....	74
5.5.4 Architecture détaillée du système.....	75
5.5.4.1 Module AnonAgent.....	75
5.5.4.1 Le Serveur Mix .....	76
5.5.5 Implémentation .....	78
5.5.5.1 Le module AnonAgent.....	78
5.5.5.2 Fonctionnement du module.....	79
5.5.5.3 Serveur mix .....	81
5.5.6 Tests .....	83
5.5.7 Conclusion .....	86
Conclusion générale.....	88
BIBLIOGRAPHIE.....	89